

541447

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 9 月 10 日 (10.09.2004)

PCT

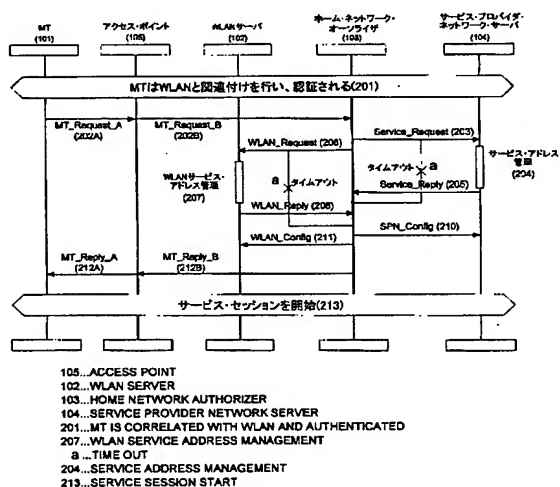
(10) 国際公開番号
WO 2004/077754 A1

- (51) 国際特許分類: H04L 12/46, 12/28 (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (21) 国際出願番号: PCT/JP2004/000176
- (22) 国際出願日: 2004 年 1 月 14 日 (14.01.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-6175 2003 年 1 月 14 日 (14.01.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1 0 0 6 番地 Osaka (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): タン ペク ユー (TAN, Pek-Yew). チェン ホン (CHENG, Hong). タン チー ビン (TAN, Chee Bing).
- (74) 代理人: 二瓶 正敬 (NIHEI, Masayuki); 〒1600022 東京都新宿区新宿 2 丁目 8 - 8 とみん新宿ビル 2 F Tokyo (JP).
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).
- 添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: SERVICE IN WLAN INTER-WORKING, ADDRESS MANAGEMENT SYSTEM, AND METHOD

(54) 発明の名称: WLAN相互接続におけるサービス及びアドレス管理システム及び方法



(57) Abstract: There is provided a solution for managing mobile terminal address allocation in a WLAN inter-working. The mobile terminal acquires permission to access a service and an address and can establish a tunnel. Moreover, in the management process, protection is performed by an appropriate encryption and no special security setting procedure is required. Furthermore, there is provided a method for acquiring an address associated with a session by utilizing the service permission procedure. Even when a terminal accesses a plurality of sessions, it is possible to hold a plurality of addresses and the address management is integrated by the policy control mechanism. Thus, after an address modification, there is provided means for the terminal and its home network to constitute a WLAN. Moreover, by using a channel usable in the procedure, QoS or tunneling information is corrected according to a new status and provided.

[続葉有]

WO 2004/077754 A1



2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

本発明によれば、WLAN相互接続における移動端末のアドレス割り当てを管理するための解決策が提供される。移動端末は、サービスへのアクセスの許可と共に、アドレスを取得してトンネルを設定することが可能となる。また、管理プロセスにおいては、特有の暗号化で保護され、特別なセキュリティの設定手続きが必要とされない。さらに、サービス許可手続きを利用して、セッションに関連するアドレスの取得を行うための方法が提供される。端末が複数のセッションにアクセスする場合でも、複数のアドレスを保持することができ、アドレス管理は、ポリシー・コントロール機構に統合される。これによって、アドレス変更後に、端末及びそのホーム・ネットワークがWLANを構成するための手段が提供される。また、その手続きで利用可能なチャネルを使用して、QoS、あるいはトネリング情報が、新たなステータスに応じて修正され、提供される。

明 細 書

WLAN相互接続におけるサービス及びアドレス管理システム及び方法

5 技術分野

本発明は、無線データ通信の分野に関する。また特に、本発明は、無線LAN（WLAN）環境において、他のネットワークから訪れるモバイル・ユーザのためのアドレス管理に関し、WLANが、例えば、別の管理ドメイン内に存在し、他の無線技術を使用する3Gネットワークや
10 WLANなどの公衆無線ネットワークとの相互接続（inter-networking）を行う際に使用可能なものである。また、本発明は、アドレス割り付け、構成、トンネリングの設定などのために、WLAN及び相互接続ネットワーク（inter-worked network）に加えて、移動端末によって利用可能であり、その結果、移動端末はWLANにおいて加入したサービス
15 にアクセス可能となる。

背景技術

WLAN相互接続（WLAN inter-working）では、端末が加入したすべてのサービスにアクセスすることができるよう、端末はアドレス付けが可能（addressable）でなければならない。サービスがIPを通じて伝
20 送される場合、端末は、あるIPアドレスに関連付けられているはずである。モバイルの世界では、端末の接続点が頻繁に変わり、端末があるアクティブなサービス・セッションの間に、いくつかのドメインを渡り歩くことが十分に起こり得る。この端末の移動性の要件を満たすために、
25 アドレス管理のメカニズムには、端末が接続点を変更するごとに、端末のアドレスを構成（configure）し更新することが要求される。

モバイルIPは、インターネット技術検討委員会（IETF）で公開されている標準化技術であり（非特許文献1）（非特許文献2）、移動端末のためのアドレス管理とトラフィックのルーティングに対する解決策を提供する。この技術によって、様々なIPネットワーク内を動き回
5 る場合に、ユーザは、同一のアドレスを使用しながら位置特定可能な状態（reachable）となる。移動性がIPレベルで管理されているので、モバイルIPは、基礎となるリンク層の技術に束縛されず、3Gのセルラ・ネットワーク、又は無線LAN（例えば、802.11のネットワーク）内の端末に対して、同一のプロトコル・スタックの適用が可能となる。
10 る。例えば、WLANと3Gのセルラ・ネットワークとの相互接続などのアクセス技術の融合において、この種の調和したレベルの解決策が、特に有用である。モバイルIPでは、IP接続によってアドレス管理が行われ、IP接続が利用可能でない場合には、アドレス管理が不可能となる。また、さらに、モバイルIPでは、端末が、ホーム・アドレスを
15 有し、かつ、そのホーム・エージェントを知っている必要がある。こうした要件は、例えば、端末が最初にフォーリンWLANで動作を開始する場合など、相互接続の動作過程では満たされないかもしれない。

また、モバイルIPv6のドラフトでは、移動ノード（mobile node）のホーム・アドレスのセッティング方法が導入されている（非特許文
20 献2）。端末は、例えば、DHCPv6（非特許文献3）を使って、まず、気付アドレス（Care of address）を最初に生成し、このアドレスを使用して、最終的なホーム・アドレスを設定するホーム・ネットワークとの通信を行う。しかし、WLANから得られた気付アドレスを使用した場合には、移動ノードのホーム・ネットワークは必ずしも位置特定可
25 能な状態とはならないので、WLAN相互接続においては、動作が不可能となる。さらに、複数回のやり取りを行うコンフィギュレーション処

理は、時間を消費するものであり、ユーザの期待に沿うものとはならない。

また、ダイアメータ・モバイル I P v 6 の適用（非特許文献 4）によって、A A A の構成に基づいて、モバイル I P v 6 のアドレス管理のための解決策が示されている。この解決策では、A A A サーバと移動先及びホーム・ネットワークのクライアントが、アドレス更新及びエージェント発見を実行することが利用されている。そのメカニズムでは、移動ノードは、例えば、ルータ・アドバタイズメント・メッセージを聞くことができるなど、メッセージ交換用のローカル I P 接続を有することが要求されるが、フォーリン・ドメインのローカル・ポリシーによって、必ずしも可能であるとは限らない。さらに、この機構は、アドレスが移動端末のホーム・ドメインに属する状況でのみ提供されるものである。W L A N 相互接続では、端末がアクセスしているサービスに依存する別のドメインからのアドレスを端末が使用することになり、このアドレスは
15 端末のサービス・リクエストの情報を持たないので、この機構は W L A N 相互接続をサポートすることはできない。この機構は、モバイル I P v 6 環境のために設計されており、したがって、モバイル I P スタックのない端末では動作不可能である。

さらに、3 G P P によって解決策、端末のアドレッシングとトンネリングとを管理するための G T P（非特許文献 5）が提供されている。G T P は、コントロール用の G T P - C、及び、ユーザ・データのトラフィック用の G T P - U の 2 つのパートを有している。G T P は、U D P 上で動作し、U D P パケット中のユーザ・データをカプセル化する。この G T P は、G P R S（非特許文献 6）ネットワーク用に設計されており、
20 例えば、G G S N、S G S N ノードなどの G P R S ネットワークの特徴に非常に依存しており、単純な無線アクセス・ネットワーク（例えば、

WLAN)への適用は困難である。

非特許文献 1 「IP mobility support for IPv4」

<http://www.ietf.org/rfc/rfc3344.txt>

非特許文献 2 「Mobility support in IPv6」

5 <http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-19.txt>

非特許文献 3 「Dynamic Host Configuration Protocol for IPv6
(DHCPv6)」

<http://www.ietf.org/internet-drafts/draft-ietf-dhc-dhcpv6-28.txt>

非特許文献 4 「Diameter Mobile IPv6 Application」

10 <http://www.ietf.org/internet-drafts/draft-le-aaa-diameter-mobileipv6-02.txt>

非特許文献 5 「GPRS Tunnelling Protocol (GTP) across the Gn and
Gp Interface (Release 5)」 3GPP TS 29.060 V5.3.0 (2002-09)

ftp://ftp.3gpp.org/Specs/archive/29_series/

15 非特許文献 6 「General Packet Radio Service (GPRS); Service
description; Stage 2 (Release 5)」 3GPP TS 23.060 V5.2.0 (2002-06)

ftp://ftp.3gpp.org/Specs/archive/23_series/

非特許文献 7 「IP Multimedia Subsystem (IMS); Stage 2 (Release 5)
」 3GPP TS 23.228 V5.6.0 (2002-09)

20 ftp://ftp.3gpp.org/Specs/archive/23_series/

非特許文献 8 「Diameter Base Protocol」

<http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-15.txt>

非特許文献 9 「PPP Extensible Authentication Protocol (EAP)」

<http://www.ietf.org/rfc/rfc2284.txt>

25 非特許文献 10 3GPP project <http://www.3gpp.org>

非特許文献 11 3GPP2 project <http://www.3gpp2.org>

非特許文献 1 2 「The Network Access Identifier」

<http://www.ietf.org/rfc/rfc2486.txt>

非特許文献 1 3 「Numbering, addressing and identification
(Release 5)」 3GPP TS 23.003 V5.3.0 (2002-06)

5 ftp://ftp.3gpp.org/Sepcs/archive/23_series/

非特許文献 1 4 「Port-Based Network Access Control」 IEEE Std
802.1X-2001 <http://standards.ieee.org/getieee802/>

非特許文献 1 5 「Diameter Extensible Authentication Protocol
(EAP) Application」

10 <http://www.ietf.org/internet-drafts/draft-ietf-aaa-eap-00.txt>

非特許文献 1 6 「Diameter NASREQ Application」

[http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-09
.txt](http://www.ietf.org/internet-drafts/draft-ietf-aaa-diameter-nasreq-09.txt)

非特許文献 1 7 「IPv6 Stateless Address Autoconfiguration」

15 <http://www.ietf.org/rfc/rfc2462.txt>

通常、WLAN及び相互接続ネットワークは、異なる管理ドメインに存在している。これは、アドレス空間が別々に管理されていることを意味している。したがって、移動端末が、そのホーム・ネットワークとは異なるドメインのWLANに移動した場合、端末への連続的なサービス
20 配送を保証するために、何らかのアドレス構成を実行しなければならない。このアドレス構成には、例えば、IPアドレス割り付け、アドレス登録、トンネリングの設定なども含まれている。

WLANを通じて端末に任意のサービスが配送されるようにするためには、アドレスの限定が行われる。例えば、WLANから3Gネットワーク内のIMS（非特許文献7）サービスにアクセスするためには、端
25 末は、IMSを提供するネットワークに属するアドレスを有する必要が

あり、結果的に、異なるサービスへの並列のアクセスを行う移動端末は、複数のIPアドレスが割り当てられるよう要求される。

WLANでは、認証及びその許可が与えられる前に、端末が、例えば、通常のデータ・パケットを送受信するなど、いかなるリソースを使用することにも許されていない。例えばMIPv6の中で示唆されるような通常の機構では、許可処理の成功後にのみアドレスの構成が行われるが、この種のアプローチは時間がかかり、いくつかのサービスにおける要件を満たすことができない。この許可処理の前にアドレス構成を行うためには、アドレス構成に関連した情報がアクセス・コントロール・メッセージに統合される必要がある。また、アドレス管理は通常、ユーザの加入情報に基づいており、移動端末のホーム・ネットワークによって管理される必要がある。しかし、任意の外部サービスにおいては、ホーム・ネットワーク以外のドメインから、アドレスが割り当てられる必要がある。この場合、ホーム・ネットワークが、アドレス割り当てやそのドメインが有する他の情報に関するやり取りを行えるメカニズムが必要となる。

また、端末がアドレスを変更する場合、その端末に関連した終端点間（エンド・トゥー・エンド）QoSが影響を受けることになる。例えば、もしアドレスが変わった場合には、送信元アドレス又は送信先アドレスの情報に基づくトラフィック・フィルタは、流れ（フロー）を正確に分類することは不可能となる。ファイア・ウォールや他のトラフィック・コントロール機能を実施するWLANについては、さらに、端末の新しいアドレスが示される必要があり、さもないと、トラフィックが妨げられるか、又は、中断されることとなる。

25

発明の開示

端末がWLANに入った場合、端末は、リソースへのアクセスを行うために、認証処理及び許可処理を完結しなければならない。本発明では、アクセス・コントロール・メカニズムに統合されるアドレス管理への解決策が示される。この統合によって、アクセスの許可と同時に、端末の
5 アドレスの割り当てが行われることが可能となる。また、端末は、アクセス・コントロール・メカニズムを再利用して拡張するので、新しいプロトコルを実施する必要はない。アドレスの構成処理は、アクセス・コントロール処理の固有の暗号化及び保護によって守られ、したがって、特別なセキュリティの設定を必要としない。

10 また、本発明は、さらに、端末のホーム・ネットワークが端末のサービスを提供するネットワークとアドレス管理の取り決めを行うための手段を提供する。この種のやり取りは、バック・エンド・プロセスであり、移動端末とWLANには明らかなもの（transparent）であり、その取り決めの結果は、サービス許可処理を利用して、WLAN及び移動端末
15 に送られることとなる。

また、並列のアクセス・セッションが同一の端末に存在する場合には、複数のアドレスが要求されることとなる。本発明では、きめ細かいサービス許可処理を使用して、端末がセッションに関連するアドレスを取得するための方法が提供される。各セッションは、関連付けられたアドレス
20 を使用して、新しいアドレスへの移行が行われる。

また、アドレス管理は、ポリシー・コントロール・メカニズムにも統合される。ポリシー・コントロールは、アドレスが変わった後、必要な場合には、端末及びそのホーム・ネットワークにWLANを構成するための手段を提供する。QoS、又は、トンネリングの情報は、既存のポリシー・コントロール処理で利用可能なチャンネルを使用した新しいステータスに従って、修正され、供給される。これによって、ローミング
25

時間内に、アドレスのスムーズな移行を達成することが可能となり、QoSの中断を最小限に抑えることが可能となる。

図面の簡単な説明

5 図1は、本発明のWLAN相互接続における移動端末のアドレスの割り当て、トンネルの設定、サービスの取り決めの管理に使用されるネットワーク構成の一例を示すブロック図、

図2は、図1に示される構成で使用する、端末のアドレスの割り当て、トンネルの設定、サービスの取り決めのためのメッセージ・シーケンスの一例を示すシーケンス・チャート、
10

図3は、図2に示されるメッセージ交換で移動端末によって使用されるメッセージの構成の一実施例を示すデータ構造図、

図4は、アドレス割り当て要求のために移動端末によって利用されるフォーマットの一例を示すデータ構造図、

15 図5は、WLAN相互接続における移動端末のアドレス割り当て、トンネルの設定、サービスの取り決めのための図1で示されるフレームワークにおけるホーム・ネットワーク・オーソライザの一実施例を示す状態遷移図、

図6は、ホーム・ネットワーク・オーソライザで要求メッセージの処理手続きを行うために使用され得るフローチャートの一例を示すフローチャート、
20

図7は、サービス・プロバイダ・ネットワーク・サーバと移動端末のサービスの詳細、アドレス割り当て、トンネル設定の取り決めを行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構成の一実施例を示すデータ構造図、
25

図8は、WLANサーバと移動端末のサービスの詳細、アドレス割り

当て、トンネル設定の取り決めを行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構造の一実施例を示すデータ構造図、

- 図 9 は、ホーム・ネットワーク・ドメイン内のポリシー・サーバの移動端末の状態に関する更新を行うために、ホーム・ネットワーク・オーソライザによって使用されるメッセージの構造の一実施例を示すデータ構造図である。

発明を実施するための最良の形態

- 10 本発明は、WLANが他のネットワークと相互接続（inter-work）するために使用されるものである。相互接続されたネットワークとしては、別のWLAN又は公衆セルラ・ネットワークが可能であり、どちらの場合においても、容易に、本発明を適用することが可能である。また、本発明は、アドレス管理や、アドレスの遷移（つまり、モビリティ・コントロール）に関連したサービス提供を行うことを目的として使用されるものである。

- ここで提案される機構（スキーム）を適用する場合には、特別なインターフェースやプロトコルを実施する必要はない。この機構は、既存のアクセス・コントロール・メカニズムを再利用し、必要な機能性を支援するために、その属性のうちのいくつかを拡張する。アドレス割り付けでは、その修正がサービス許可手続きに統合される。許可手続きが、認証から得られた信頼によって暗号化され保護されるので、アドレス情報も同一のセキュリティ・レベルで保護され、許可情報の一部として示されて、通常の許可情報と同一の方法で転送可能となる。例えば、AVPに特有の許可としてダイアメータ（非特許文献 8）に含まれたり、EAP方法による許可が利用可能な場合には、EAP（非特許文献 9）の属

性として含まれたりすることが可能である。

端末がWLANに入った場合には、サービスを利用することが認められる前に、認証及び許可が行われる。許可手続きでは、端末が、アクセスしようとするサービスを要求し、この情報はWLANを通じて端末の
5 ホーム・ネットワークに渡される。端末のホーム・ネットワークは、ユーザの加入者プロフィールに基づいてサービスを許可すべきか否かを決定する。さらに、要求されたサービスに応じて、端末のホーム・ネットワークは、サービスに使用されるアドレスを決定する。例えば、IMSサービスについては、アドレスはIMSアドレス空間から割り当てられ
10 る必要があり、一方、ローカルWLANサービスについては、ローカルで取得されたアドレスで十分である。また、さらに、アドレス管理に関連するトンネリングの情報の確認が行われる。

アドレス情報は許可情報に含まれ、許可成功メッセージと共に送られる。この情報の一部は、WLANに送られ、一部は、通常の許可手続き
15 と同様、端末に送られる。例えば、端末が端末自体のアドレス構成を行えるようにするために、アドレスが端末に送られる必要がある。また、もしネットワーク・トンネリングが必要な場合には、WLANによって、トンネリングの情報が使用される。

また、アドレスの変更が必要な場合には、サービス許可の詳細な手続き
20 きを行わずに、迅速な更新を行うために、再許可手続きを利用することが可能である。

また、端末がサービスへのアクセスを開始した場合に、ポリシー・コントロールが開始される。アドレス情報は、端末のホーム・ネットワークのポリシー・サーバによって利用可能となり、その後、ポリシー・サーバは、ポリシー決定をアドレス情報に基づいて行うことが可能となる。
25 また、アドレスの変更時には、ポリシー・サーバに対して、対応するポ

リシーを更新するよう通知が行われ、その結果、QoS及びサービス提供が保証される。

発明の理解を支援するため、次の定義が使用される。

「WLAN」は、無線のローカル・エリア・ネットワークを指すものであり、無線技術を通じて移動端末にLANサービスを提供するための任意の数の装置を含むものである。

「3Gネットワーク」は第3世代の公衆アクセス・ネットワークを指すものであり、例えば、3GPP（非特許文献10）や3GPP2（非特許文献11）によって定義されるシステムである。

10 「移動端末」は、無線技術によってWLAN及び他のネットワークによって提供されるサービスへのアクセスに使用される装置を指すものである。

「ホーム・ネットワーク」は、移動端末（MT）のサービス加入情報が格納されているネットワークを指すものであり、相互接続のシナリオでは、MTが最初に加入したネットワーク、又は、MTの加入情報に完全
15 にアクセスすることが許可されている訪問先のネットワークである。

「サービス・プロバイダ・ネットワーク」は、MTが要求したサービスが提供されるネットワークを指すものであり、例えば、ホーム・ネットワーク、WLAN、外部ネットワークなど、任意のネットワークが可能
20 である。

「ネットワーク・エレメント」は、情報処理を実行することが可能なネットワーク内で機能している任意の装置を指すものである。

「ポリシー・サーバ」は、ネットワーク・ドメインのポリシー・コントロール機能を実行するネットワーク・エレメントを指すものである。
25 ポリシー・コントロール機能は、例えば、ローカルのリソース配分、パケット・フィルタの更新、ルーティングの更新などを含んでいる。

「エア・インターフェース」は、移動端末がWLANにアクセスするための任意の無線アクセス技術を指すものである。

「ストリーム」は、ある属性を共通に持っているネットワーク内で転送されるパケットの集まりである。

- 5 「トラフィック」は、ネットワーク内で転送されるストリームの集まりである。

「フロー」は、データ・パス、及び、ストリームを伝送するために使用されるデータ・パスに必要とされるネットワーク・リソースを指すものである。

- 10 「QoS」は、データ・ストリーム又はトラフィックのサービス品質 (Quality of Service) の用語を指すものである。

「メッセージ」は、相互接続をコントロールする目的で、ネットワーク・エレメント間で交換される情報を指すものである。

- 15 「オペレーション・シーケンス」は、相互接続コントロールのために、任意のネットワーク・エレメント間での一連のメッセージ交換を指すものである。

「上位レイヤ」は、現在のエンティティの上に存在し、現在のエンティティから渡されたパケットを処理するすべてのエンティティを指すものである。

- 20 「クライアントに基づくトンネル」は、トンネルの終端点のうちの1つが移動端末であるトンネリング機構を指すものである。

「ネットワークに基づくトンネル」は、トンネルの終端点が移動端末以外のネットワーク・エレメントに存在するトンネリング機構を指すものである。

- 25 以下の記述では、本発明を完全に理解するための説明において、具体的な数、時間、構造、プロトコルの名前、その他のパラメータが使用さ

れるが、このような具体的な詳述がなくても、本発明の実施が可能なことは当業者にとって明白である。また、よく知られた構成要素やモジュールに関しては、本発明を不必要に不明瞭なものとしないうブロック図で示されている。

- 5 端末が高度な移動性を有するという特性により、モビリティ・コントロールは、WLAN相互接続における最も顕著な問題のうちの1つである。端末が移動する場合、端末は、接続点に局所的（ローカル）でないアドレスを使用するよう要請されている。例えば、WLANに入り込んだ3G端末に関しては、そのホーム・ネットワークのサービス（例えば、
- 10 IMSサービス）にアクセスするためには、3Gドメインのアドレスが必要とされる。端末が、3Gネットワーク内にあるサービスを開始した場合、アドレスは、例えば、GPRSサービス（非特許文献6）などの3Gのスキームに従って割り当てられ、このアドレスは、端末の3Gセルラ・インターフェースに関連付けられる。また、端末がWLANDメ
- 15 インに入る場合には、高いスループットを実現することができるので、そのWLANインターフェースを使用して通信することが望まれる。例えば、2重のインターフェース（GPRS及びIEEE802.11）を備えたPDAは、道路上ではGPRSインターフェースを使用し、ホット・スポット内ではIEEE802.11インターフェースを使用す
- 20 ることが望まれる。端末がWLANインターフェースを使用して3Gサービスにアクセスする場合には、端末は、3Gインターフェースから得られたものと同一のアドレスを使用し続ける必要がある。そうでなければ、端末はサービス中断に直面し、セッションを再度初期設定しなければならず、これは、ユーザにとって望ましいことではない。また、使用
- 25 中のアドレスはWLANに局所的ではないので、トンネルは、端末からサービス・プロバイダ・ネットワークまで設定されなくてはならない。

図1には、アドレス割り付けとトンネルのセット・アップのための本発明の実施例が示されている。なお、混乱を避けるため、シグナリングに参加するネットワーク・エンティティのみが図示されている。

移動端末(101)はネットワークからあるサービスを要求するエンティティである。実際には、例えば、Bluetoothリンクによってラップトップ・コンピュータに接続されたハンドセットなどのように、いくつかのエンティティを有することが可能であるが、単純化のため、図1には1つのセットとして描かれている。WLAN機能(WLAN function)(1001)内において、アクセス・ポイント(105)は、移動端末(101)に対してWLANアクセスを提供するエンティティである。移動端末(101)がWLANサービスを利用する許可が与えられるまで、アクセス・ポイント(105)は、移動端末(101)からのデータ・トラフィックをすべて遮断するが、ある特定のデータ・パケットのみを許可するコントロール・チャンネルが、アクセス・コントロール・シグナリングを行うために開いた状態(open)となる。移動端末(101)は、無線リンク(1011)を通じてアクセス・ポイント(105)と通信を行う。このリンクとして、例えば、IEEE 802.11、HipерLAN/2、赤外線などを始め、どのような種類の無線技術を使用することも可能であり、同様のアクセス・コントロール技術が適用可能な場合には、このリンクにおいて、例えば光ファイバなどの他の技術を使用することも可能である。また、WLAN管理サーバ(WLANサーバ)(102)が、WLAN内の別のエンティティとして存在している。このWLANサーバ(102)は、アドレス空間の管理及びWLANのリソース管理を担当しており、WLANのゲートウェイ上に存在するか、単純なWLANではアクセス・ポイント(105)に共設されている。WLANサーバ(102)は、インターフェース(1015)

を介して、アクセス・ポイント（１０５）と通信を行う。これは、例えばエア・インターフェースを介するＱoSの管理など、WLANリソース・コントロールやサービス提供のためのものである。また、WLANを管理するため、このサーバは、例えば、不図示のWLANゲートウェイやファイア・ウォールなど、WLANの他のエンティティとの相互作用を行うことも可能である。

端末のホーム・ネットワーク（１００２）では、ホーム・ネットワーク・オーソライザ（Home Network Authorizer）（１０３）がサービス許可及びアドレス割り付けの管理を行う。アクセス・ポイント（１０５）及びWLANサーバ（１０２）は両方とも、リンク（１０１２）及びリンク（１０１４）を介して、サービス制御情報を取得するためにホーム・ネットワーク・オーソライザ（１０３）とそれぞれ通信を行う。なお、物理的に、リンク（１０１２）及びリンク（１０１４）を同一とすることも可能であり、すなわち、同一のプロトコルを使用し、同一の端末間で、同一の packets にカプセル化された場合でも、それらは、論理上分離される。

移動端末（１０１）は、それが加入しているすべてのサービスを要求することが可能である。これらのサービスは、ホーム・ネットワーク（１００２）、個別のサービス・プロバイダ・ネットワーク（１００３）、又は、WLAN自体にあるかもしれない。サービスが、ホーム・ネットワーク（１００２）又はWLANによって提供される場合には、サービス・プロバイダ・ネットワーク（１００３）は、これらのネットワークとオーバラップすることになり、コントロール機能を両方に関連付けることが可能となる。また、サービス・プロバイダ・ネットワーク管理サーバ（サービス・プロバイダ・ネットワーク・サーバ）（１０４）は、サービス許可及びサービス・プロバイダ・ネットワーク（１００３）の

- アドレス割り付けを管理する。ホーム・ネットワーク・オーソライザ（
103）は、コントロール・インターフェース（1013）を介して、
サービス・プロバイダ・ネットワーク・サーバ（104）と通信を行う。
実際には、サービス・プロバイダ・ネットワーク（1003）として、
5 WLAN、ホーム・ネットワーク（1002）又は別のネットワークを
利用することが可能である。また、サービスが、ホーム・ネットワーク
（1002）で提供される場合には、このインターフェースは内部イン
ターフェースとなり、正確なフォーマットや、後述の実施例に記述され
るものと同一のプロトコルを使用する必要はない。
- 10 図2は、上記のフレームワークを使用して、WLAN相互接続のアド
レス管理のためのオペレーション・シーケンスの一例を示すものである。
なお、この動作では、移動端末（MT）（101）がすでに、WLAN
の関連付け及び認証手続き（201）を終了していると仮定する。すな
わち、移動端末（101）とアクセス・ポイント（105）は、相互に
15 認証し合っており、以降のメッセージ交換のための暗号化による保護が、
すでに行われている。移動端末（101）は、WLANを通じて任意の
サービスにアクセスしたい場合には、リンク（1011）を介して、ア
クセス・ポイント（105）にMT_Request_Aメッセージ（202A）
を送信し、そのメッセージは、ホーム・ネットワーク・オーソライザ（
20 103）に届けられる。このメッセージは、認証手続き（201）から
生成されたキーによって、終端点間（エンド・トゥー・エンド）で保護
されている。図3は、メッセージMT_Request_Aメッセージ（202A
）の実施例を示している。

- メッセージはMessage_Typeフィールド（301）から始まる。この
25 フィールドは、例えば、要求、返答など、どの種類のメッセージがカプ
セル化されているかを識別する。このフィールドの長さは1オクテット

であり、メッセージ・タイプは整数番号によって表わされる。これは、エア・インターフェースを通じたシグナリングに対して制限されたリソースを節約するものである。なお、必要な場合には、このフィールドが他のフォーマットも採用できることは当業者にとっては明白である。

- 5 Message_Typeフィールド（3 0 1）に続いて、Message_Lengthフィールド（3 0 2）が存在する。これは、Message_Typeフィールド（3 0 1）を含む全体のメッセージの長さに関する情報を含んでいる。また、次のフィールドは、Domain_Nameフィールド（3 0 3）である。このフィールドは、移動端末（1 0 1）のホーム・ドメインを識別する。なお、ネットワーク・アクセス識別子（Network Access Identifier : N A
- 10 1）（非特許文献 1 2）を使用することも可能であり、この場合には、例えば「UserID@home.domain.3gpp.org」の形式となる。ユーザの識別情報を保護するため、「@」記号の前のUserID部分は、例えば「roamed」などのワイルドカード値を使用する。ホーム・ドメイン情報は、移動
- 15 端末（1 0 1）のホーム・ネットワーク・オーソライザ（1 0 3）に対して、メッセージをルーティングするために使用される。

- 上記の 3 つのフィールド、Message_Typeフィールド（3 0 1）、Message_Lengthフィールド（3 0 2）及びDomain_Nameフィールド（3 0 3）は、移動端末（1 0 1）とアクセス・ポイント（1 0 5）との間のセキュリティの関連付けによって保護される。このセキュリティの関連付けは、エア・インターフェースの保護のための認証手続き（2 0 1）から得られる。したがって、目的を達成するために、アクセス・ポイント（1 0 5）が、これらのフィールドに含まれている情報にアクセスすることが可能である。Domain_Nameフィールド（3 0 3）に続
- 20 くフィールドは、移動端末（1 0 1）とホーム・ネットワーク・オーソライザ（1 0 3）との間のセキュリティの関連付けによって保護される。

例えば、これには、ホーム・ネットワーク・オーソライザ（１０３）のパブリック・キーが可能であり、すなわち、認証手続き（２０１）に由来したセッション・キーである、また、メッセージ保護のために使用されるキーのインデックスを示すために、Domain_Nameフィールド（３
5 ０３）のUserID部分を使用することも可能である。

Domain_Nameフィールド（３０３）の後には、MT_IDフィールド（３
3 ０４）が存在する。このフィールドは、ホーム・ネットワーク（１０
0 ２）のコンテキストにおいて、移動端末（１０１）を一意に識別する
ための情報を含んでいる。これは、例えば、移動端末（１０１）のIM
10 S I（非特許文献１３）、又は、認証手続きで獲得されたTMS I（非
特許文献１３）が可能である。ホーム・ネットワーク・オーソライザ（
1 ０３）は、ユーザの加入情報を検索するため、この識別子を利用する。
ホーム・ネットワーク・オーソライザ（１０３）が実際のユーザ識別情
報にそれをマッピングすることができる限り、このフィールドに他のフ
15 ォーマットを使用することも可能であることは、当業者にとっては明白
である。

次のフィールドはService_Requestフィールド（３０５）である。こ
のフィールドは、ホーム・ネットワーク・オーソライザ（１０３）に対
してアクセスすることを望むサービスを示すため、移動端末（１０１）
20 によって使用される。メッセージは、移動端末（１０１）とそのホーム
・ネットワーク・オーソライザ（１０３）との間のものなので、これは、
特定のオペレータ及びネットワークに特有のものである。例えば、３Ｇ
PPネットワークでは、これは、使用するGGSN及びアクセスする特
別のサービスを識別するためのAPN（非特許文献１３）であり得る。
25 ホーム・ネットワーク（１００２）が別のタイプである場合には、他の
フォーマットを使用することが可能であることは、当業者にとって明白

- である。さらに、例えば、帯域幅の要求など、他のサービス・リクエスト情報を追加することも可能である。フィールドに利用可能な値としては、「2M.bandwidth.request.IMS.foo.bar.operator.name.operator.group.gprs」があり得る。「request」の後の部分は、サービスを識別する標準のAPNであり、また、「request」の前の部分は、特定のサービス・リクエストである。実際のリクエスト属性は、サービスに依存しており、また、オペレータが定義することも可能である。移動端末（101）は、SIM又はUSIMカードから、フォーマットに関する情報を獲得することが可能である。
- 10 また、Session_IDフィールド（306）はセッション制御情報を提供する。これは、移動端末（101）が、このサービスの要求がホーム・ネットワーク・オーソライザ（103）に関連するセッションであることを識別するために使用される。セッションの識別子は、移動端末（101）内では局所的に一意であるべきであり、移動端末（101）は、
- 15 すべてのサービス・セッションのローカルな記録を維持すべきである。新しいサービス・セッションがスタートする場合は常に、新しいセッション識別子を備えた新しいエントリが作られ、セッションが終了する場合には、そのエントリは削除されて、識別子は解放されて再利用可能となる。本実施例では、フィールドは2オクテットであり、また、識別子
- 20 は16進数の値である。なお、端末にサポートされた他のタイプの識別子の使用が可能なことは、当業者にとっては明白である。MT_IDフィールド（304）及びSession_IDフィールド（306）は、ホーム・ネットワーク・オーソライザ（103）において、サービス・セッションを一意に識別する。
- 25 また、Address_Requestフィールド（307）は、移動端末（101）からのアドレス割り付けの要求に関する情報を含んでいる。本実施例

では、図4に示されるように、複合した構造が使用されている。この構造の第1のパートは、Address_Typeフィールド(401)である。これは、どのタイプのアドレスが移動端末(101)にサポートされているかを識別する。このフィールドのサイズは1オクテットであり、可能な
5 値は次の通りである。

No_IP::=0x00;

Single_Stack_IPv4::=0x01;

Single_Stack_IPv6_FullAddress::=0x02;

Single_Stack_IPv6_Prefix::=0x03;

10 Dual_Stack_IPv4_Preferred::=0x04;

Dual_Stack_IPv6_Preferred_FullAddress::=0x05;

Dual_Stack_IPv6_Preferred_Prefix::=0x06

さらなるタイプがサポートされ、他の数が使用され得ることは、当業者にとっては明白である。また、この構造の第2のパートは、

15 Suggestion_Lengthフィールド(402)である。このフィールドは、次のフィールドAddress_Suggestionsフィールド(403)の長さを示している。Address_Suggestionsフィールド(403)は、移動端末(101)が割り当てられることを望むアドレスを列挙する。例えば、進行中のセッションが、あるアドレスを使用している場合、そのセッションが中断されないように同一のアドレスが割り当てられることが重要である。例えば、Address_Suggestionsフィールド(403)は、アドレスのリストである。リスト内の各エントリは、例えば、IPv4やIPv6などのアドレスのタイプを示す1オクテットのタイプ・フィールドから始まり、実際のアドレスがそれに続く。端末によるアドレス提示の
20 特徴をサポートしないホーム・ネットワーク・オーソライザ(103)では、Suggestion_Lengthフィールド(402)及び

Address_Suggestionsフィールド（４０３）は、暗黙のうちに無視される。

また、Address_Requestフィールド（３０７）の後には、
Tunnel_Requestフィールド（３０８）が存在する。このフィールドは、
5 どのタイプのトンネルをサポートしているかを示すために、移動端末（
101）によって使用される。このフィールドの最初のオクテットは、
それ自体を含むこのフィールドの長さを示し、このフィールドの内容は、
2オクテットを占める各エントリを持つリストとすることが可能である。
各エントリの最初のオクテットは、移動端末（１０１）がサポートする
10 トンネル・タイプの識別子を含んでおり、そのオクテットの値には、次の
ものが可能である。

ネットワーク・トンネル -- 一般的::=0x01;
ネットワーク・トンネル -- モバイルIPv4::=0x02;
クライアント・トンネル -- 一般的::=0x04
15 クライアント・トンネル -- モバイルIPv4::=0x05;
クライアント・トンネル -- モバイルIPv6::=0x06;
トンネル無し::=0x08

このフィールドで、他のトンネルのタイプを定義して使用できることは、当業者にとっては明白である。また、各エントリの２番目のオクテットは、トンネルの方向を示している。このオクテットの可能な値は。
20 次の通りである。

トンネル -- 端末から::=0x01;
トンネル -- 端末に::=0x02;
トンネル -- 双方向::=0x03;
25 リスト内の最初のエントリは、移動端末（１０１）の好ましいタイプを示している。

また、MT_Request_Aメッセージ（202A）内の次のフィールドは
WLAN_IDフィールド（309）である。これは、ホーム・ネットワー
ク・オーソライザ（103）に対するWLANを識別する情報を含んで
おり、これによって、ホーム・ネットワーク・オーソライザ（103）
5 は、位置に基づく決定を行ったり、移動端末（101）への位置に基づ
くサービスを提供したりすることが可能となる。WLAN_IDは、認証手
続きや、例えばIEEE802ネットワークにおけるSSIDなどのア
クセス・ポイント（105）からブロードキャストされた情報から取得
可能である。さらに、移動端末（101）のローカルの識別子も含まれ
10 ている。これは、アクセス・ポイント（105）が端末を識別するた
めのものである。

また、最後のフィールドは、Security_Field（310）である。この
フィールドは、メッセージを保護するための情報を含んでいる。このフ
ィールドのために使用される正確なアルゴリズムは、移動端末（101）
15 ）とそのホーム・ネットワーク・オーソライザ（103）との間で交渉
される。また、これは、ユーザの加入時間で決定されてもよく、端末の
SIM又はUSIMカードに格納されてもよい。また、さらにソフトウ
ェア・モジュールとして実施可能であり、必要な場合には常にダウンロ
ードされるようにすることが可能である。

20 なお、MT_Request_Aメッセージ（202A）内のフィールドは、上
述のような正確なシーケンスに従う必要はなく、例えば、実際には、最
前部にフィールドの識別子を配置する限り、任意の順にフィールド（3
04）からフィールド（309）を配置することが可能である。

実際には、任意の適切なメカニズムを使用して、リンク（1011）
25 を通じてメッセージを伝送することが可能である。例えば、IEEE8
02.11ネットワークでは、IEEE802.1xに定義されるEA

POLを使用し、EAPメッセージとして実現することが可能である（非特許文献14）。

アクセス・ポイント（105）がこのメッセージを受け取った場合には、Domain_Nameフィールド（303）からホーム・ドメイン情報を
5 引き出し、例えば、DNSの照会を行なうなど、そのドメイン情報を利用して、ホーム・ネットワーク・オーソライザ（103）のアドレスを取得することが可能である。アクセス・ポイント（105）は、この情報に従って、対応するホーム・ネットワーク・オーソライザ（103）にメッセージを転送する。例えば、WLANがセントラルAAAサーバ
10 を有する場合には、アクセス・ポイント（105）は、AAAサーバにメッセージを直接転送する。そして、WLANのAAAサーバはドメイン情報を解析し、実際のホーム・ネットワーク・オーソライザ（103）にメッセージを転送する。なお、アクセス・ポイント（105）とホーム・ネットワーク・オーソライザ（103）との間に、安全なリンク
15 が存在することを前提としており、これは、認証手続き（201）での設定で可能となるか、又は、そのプロセスに由来するセキュリティの関連付けを動的に設定することによって可能となる。

また、アクセス・ポイント（105）は、メッセージ処理に参加する必要がなく、したがって、メッセージを解析するためにスタック全体を
20 実施する必要がない。それは、単にメッセージ・タイプを読み、MT_Request_Bメッセージ（202B）のステップとして示される再カプセル化及び転送を行う必要があるだけである。転送のために使用されるプロトコルとしては、任意の適切なAAAプロトコル（例えば、ダイアメタのためのEAPアプリケーション（非特許文献15）や、ダイアメタのためのNASREQアプリケーション（非特許文献16））
25 が可能である。それらのプロトコルは、認証を目的として、アクセス・

ポイント（１０５）において、すでに利用可能である。したがって、メッセージMT_Request_Aメッセージ（２０２Ａ）は、終端点間の認証手続き（２０１）と同様、本質的には、移動端末（１０１）からホーム・ネットワーク・オーソライザ（１０３）にエンド・トゥー・エンドで送
5 られる。

また、図５は、ホーム・ネットワーク・オーソライザ（１０３）の状態マシンの実施例を示すものである。ホーム・ネットワーク・オーソライザ（１０３）は、初期状態（５０１）から始まり、遷移（/intiate()）（５００１）で初期化（）の処理を行ってアイドル状態（５０２）に移
10 る。初期化（）プロセスは、他のバックエンド・サーバとの接続、セキュリティの関連付けなどを確立するために必要なすべてのステップを含んでいる。実際には、設定に依存して他のプロセスが含まれ得ることは、当業者にとっては明白である。

ホーム・ネットワーク・オーソライザ（１０３）が、遷移（５００２）
15 ）でアクセス・ポイント（１０５）から転送されたMT_Request_Bメッセージ（２０２Ｂ）を受け取った場合には、メッセージ復号状態（５０３）に遷移する。図６は、メッセージ復号状態（５０３）の実施例を示すものである。メッセージ復号状態（５０３）では、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６００１）でDomain_Name
20 フィールド（３０３）によって識別されたキーを使用して、MT_Request_Bメッセージ（202B）内のフィールドを復号する。ステップ（６００２）において、メッセージが破損されているか、又は、Security_Field（３１０）を使用して修正されていることを検知した場合、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６
25 ０１３）において、不正なメッセージのフラグをセットし、状態マシンは、遷移（５００４）でサービス却下状態（５０４）に遷移する。

MT_Request_Bメッセージ（202B）から、ホーム・ネットワーク・オーソライザ（103）は、ステップ（6003）において、MT_IDフィールド（304）から端末の識別情報に関する情報を獲得することが可能である。この識別情報を使用して、ホーム・ネットワーク・オーソライザ（103）は、そのデータベースやバックエンド・サーバ（例えば、3GPPネットワークのHSS）から、ユーザの加入情報を検索する。また、ホーム・ネットワーク・オーソライザ（103）は、さらにステップ（6004）で、Service_Requestフィールド（305）から得られたサービス要求情報を解析する。サービス要求は、例えば、帯域幅、遅れ、不安定性など、挿入される様々なサービス固有情報を含むことが可能である。ステップ（6005）において、ホーム・ネットワーク・オーソライザ（103）内では、ユーザ加入情報を使用して、ユーザにサービスを与えないでおくべきかどうかに関する決定が下される。ユーザの加入に基づいて、要求されたサービスが与えられるべきではないとされた場合、ホーム・ネットワーク・オーソライザ（103）は、ステップ（6013）において、サービスを否定するフラグをセットし、状態マシンは、遷移（5004）でサービス却下状態（504）に遷移する。もしサービスが許される場合には、ホーム・ネットワーク・オーソライザ（103）は、ステップ（6007）において、Session_IDフィールド（306）において受信したセッション識別子のサービスの端末を求めて、そのレコードを探索する。同一セッション識別子を有するレコードが存在する場合には、これがハンドオーバーの要求であることを意味し、端末には同じアドレスが割り当てられるべきである。これにより、サービス・セッションは中断されることがなくなる。また、レコードが存在しない場合には、それは新しい要求であることを意味し、ステップ（6008）において、レコード・エントリが生成され、ホーム・

ネットワーク・オーソライザ（１０３）の格納部に格納されるか、例えば、HSSなどのバックエンド・データベースが更新される。ホーム・ネットワーク・オーソライザ（１０３）は、さらにサービス情報を使用して、サービス・プロバイダ・ネットワーク（１００３）を識別し、サービス・プロバイダ・ネットワーク・サーバ（１０４）との接続がセット・アップされる。

ステップ（６００９）において、Address_Requestフィールド（３０７）から、ホーム・ネットワーク・オーソライザ（１０３）は、移動端末（１０１）が使用を望んでいるアドレスを取得する。なお、ホーム・ネットワーク・オーソライザ（１０３）が、オペレータのポリシーやその他によって、この機能をサポートしたくない場合、この情報を暗黙に無視することが可能である。移動端末（１０１）は、ホーム・ネットワーク・オーソライザ（１０３）から割り当てられた最終的なアドレスを常に使用するべきである。ホーム・ネットワーク・オーソライザ（１０３）は、要求されたサービスから、アドレスが、局所的に又はホーム・ネットワーク（１００２）内で割り当てられるべきか、あるいは、サービス・プロバイダ・ネットワーク（１００３）内で割り当てられるべきかを決定する。例えば、ユーザがWLANローカル・サービスを利用することしか認められていなければ、アドレスはWLAN内で割り当てられ、一方、VPNサービスに加入するユーザには、そのVPN内のアドレスを用いて割り当てられるべきである。

また、ホーム・ネットワーク・オーソライザ（１０３）は、ステップ（６０１０）でTunnel_Requestフィールド（３０８）から、移動端末（１０１）にサポートされたトンネルのタイプを検索する。この情報は、サービス提供のためにトンネルをセット・アップするために用いられる。移動端末（１０１）は、１つ以上のトンネルのタイプを列挙し、リスト

中の最初のを好ましいタイプのものとするのが可能である。ホーム・ネットワーク・オーソライザ（１０３）は、サービス・プロバイダ・ネットワーク・サーバ（１０４）と共にチェックを行って、どのタイプを使用すべきであるか決定する必要がある。なお、例えば、トンネル
5 の方向などの付加的な情報が含まれてもよい。

ステップ（６０１１）において、ホーム・ネットワーク・オーソライザ（１０３）は、WLAN_IDフィールド（３０９）から、移動端末（１０１）が現在関係している無線LANの識別情報を得る。この情報を使用して、ホーム・ネットワーク・オーソライザ（１０３）は、対応する
10 WLAN管理サーバ（１０２）を見つける。なお、ローミングの協定の一部として、ホーム・ネットワーク・オーソライザ（１０３）のデータベースにこの情報を格納することが可能であり、また、バックエンド・サーバ（例えばHSS）からこの情報を引き出せるようにすることも可能である。サーバの情報を取得した後、安全なリンクが確立される。こ
15 のリンクは、以降のサービス・メッセージ・シグナリングのために使用されるものである。

すべての情報を取得した後、ホーム・ネットワーク・オーソライザ（１０３）は、Service_Requestメッセージ（２０３）及びWLAN_Requestメッセージ（２０５）を作成し、ホーム・ネットワーク・オーソライザ
20 （１０３）の状態マシンが待機状態（５０４）に遷移する場合、このメッセージが送り出される。

図７は、Service_Requestメッセージ（２０３）の実施例を示すものである。このメッセージは、Home_Network_IDフィールド（７０１）から始まる。このフィールドは、移動端末（１０１）のホーム・ネットワーク識別子に関する情報を含み、オペレータの名前や大きなネットワークのサブシステムであり得る。識別子はグローバルにユニークでなけ
25

- ればならず、例えば「network.operator.3gpp.org」などのネットワークのDNS名は、この識別子の好適な候補である。ホーム・ネットワーク情報の存在によって、サービス・プロバイダ・ネットワーク・サーバ（104）は、例えば、ローミングの協定などのネットワーク・ポリシーを、サービス要求に対して適用することが可能となる。また、ユーザのプロファイルはホーム・ネットワーク（1002）によって管理されている。したがって、ユーザ情報は、サービス・プロバイダ・ネットワーク・サーバ（104）に送られるべきではないが、サービスのよりよいコントロールを可能にするため、メッセージにユーザ・プライオリティ／グルーピング情報を付加することも可能である。これは、例えば、「goldmember.network.operator.3gpp.org」などのように、ホーム・ネットワーク識別子と関連付けられてもよい。サービス・プロバイダ・ネットワーク・サーバ（104）は、これを用いて、サービスを与える場合にユーザを差別化することが可能となる。
- 15 また、次のフィールドはMT_IDフィールド（702）である。このフィールドは、移動端末（101）の識別子に関する情報を含んでおり、ホーム・ネットワーク・オーソライザ（103）がサービス・トラッキングを行うために使用される。識別子は端末のIMS I、又は、ホーム・ネットワーク・オーソライザ（103）によって割り当てられ、サービス・セッションに固有の一時的なIDであり得る。なお、この情報は、サービス・セッションが終了するまで一貫性を有している必要がある。
- 20 また、上記のフィールドに続いて、Session_IDフィールド（703）が存在する。これは、端末によって割り当てられたセッション識別子である。サービス・プロバイダ・ネットワーク・サーバ（104）は、現在行われているすべてのセッション情報の記録を保持すべきである。したがって、セッション識別子がデータベースに存在する場合には、それ
- 25

は、サービス要求がハンドオーバによって引き起こされることを意味し、また、サービスの中断を避けるために同一のアドレス構成を使用すべきであることを意味する。例えば、セッションが稼動している（アクティブ）場合、サービス・プロバイダ・ネットワーク・サーバ（104）は、
5 移動端末（101）に対して同一のアドレスを割り当てるべきである。その結果、コレスポンデント・ノードとの通信はシグナリングなしで継続されるようにすることが可能となる。

また、Address_Requestフィールド（704）は、MT_Request_Aメッセージ（202A）のものと同一である。この部分は、例えば、IP
10 v6などの割り当てるべきアドレスのタイプをサービス・プロバイダ・ネットワーク・サーバ（104）に示すものである。さらに、MT_Request_Aメッセージ（202A）のAddress_Requestフィールド（307）と同様に、移動端末（101）によって要求されたアドレスを提供する。なお、サービス・プロバイダ・ネットワーク・サーバ（1
15 04）がこの機能をサポートしたくない場合には、この情報を無視すればよい。また、ホーム・ネットワーク・オーソライザ（103）によってサービス・プロバイダ・ネットワーク（1003）からアドレスを割り当てられる必要がないと決定された場合には、このフィールドは省略されてもよい。

20 Service_Specフィールド（705）は、複合したフィールドであり、ユーザの加入情報に基づいてホーム・ネットワーク・オーソライザ（103）から要求される特定の要件に関する情報を含んでいる。このフィールドの可能な実施例（データ構造1）は、以下に示される。

```
struct Service_Spec{  
25         u_long  bitrate_avg;  
         u_long  bitrate_max;
```

```
int deliver_order;
int MTU_size;
double delay;
double jitter;
5 int priority;
int service_direction;
int QoS_type
struct timeval start_time;
struct timeval end_time;
10 };
```

この属性のうち、bitrate_avg及びbitrate_maxは、要求されたサービスを保証するビット・レート及び最大のビット・レートである。また、deliver_orderの属性は、配送が順番に行われるかどうかを示すものである。また、MTU_sizeは、サービスのために転送される最大のデータ・

15 ユニット・サイズを特定するものである。また、delayとjitterのフィールドは、サービスのためのいくつかの基本的なQoSの属性を指定するものである。また、priorityの属性は、このサービスのためのデータ・トラフィックの取り扱い優先度を示すものである。また、

service_directionの属性は、サービスが一方向か双方向かを示すものである。また、QoS_typeの属性は、例えばDiffServ、あるいはRSVPな

20 どを備えたInterServサービスなどのサービスを提供するために用いられるQoSのスキームを示すものである。また、start_time及び

end_timeは、サービスの開始時間及び終了時間を示すものである。サービス・プロバイダ・ネットワーク・サーバ（104）は、この情報を用

25 いて、サービスのためのリソースのスケジュールを決めることが可能である。なお、実際に実施される際の構造においては、サービスに固有の

他の属性が含まれてもよいことは、当業者にとっては明白である。

また、Service_Specフィールド（705）の後には、Tunnel_Specフィールド（706）が存在する。このフィールドはトンネル情報を含んでおり、MT_Request_Aメッセージ（202A）のTunnel_Requestフィールド（308）と同様だが、いくつかの特別な情報が付加されている。例えば、ネットワーク・トンネル・エントリに関しては、WLANの終端点が提供され、端末のトンネルに関しては、データ暗号化のために、セキュリティ・キーを付加することが可能である。

また、Service_Requestメッセージ（203）の最後のフィールドは、Security_Field（707）である。このフィールドは、ホーム・ネットワーク・オーソライザ（103）とサービス・プロバイダ・ネットワーク・サーバ（104）との間のセキュリティの関連付けを用いて、メッセージ全体を保護するために使用される。なお、ここで使用される正確なアルゴリズムは、実際の実施形態に依存する。

なお、Service_Requestメッセージ（203）内のフィールドが記述された順序である必要がないことは、当業者にとっては明白であり、実際には、ホーム・ネットワーク・オーソライザ（103）及びサービス・プロバイダ・ネットワーク・サーバ（104）は、シグナリングの最適化のために、任意の適切な順序の交渉を行うことも可能である。

サービス・プロバイダ・ネットワーク・サーバ（104）は、Service_Requestメッセージ（203）を受け取った後、サービス・アドレス管理（204）手続きを行なう。この手続きでは、サービス・プロバイダ・ネットワーク・サーバ（104）が、Session_ID（703）に含まれていたセッション識別子を求めて、そのデータベースの探索を行う。同一の移動端末（101）のセッション識別子が存在する場合、サービス・プロバイダ・ネットワーク・サーバ（104）は、例えば、

MTのアドレス、サービスの詳細など、その記録内のすべての情報をコピーし、それを返答メッセージとしてホーム・ネットワーク・オーソライザ（103）に直接返信する。

また、セッション識別子が存在しない場合には、サービス・プロバイダ・ネットワーク・サーバ（104）は、そのデータベースの指標（インデックス）として、新しいセッション識別子を使用して新しいエントリを作成する。サービス・プロバイダ・ネットワーク・サーバ（104）は、Address_Requestフィールド（704）をチェックし、このフィールドで指定されたアドレスのタイプに基づいて、移動端末（101）に適切なアドレスを割り当てる。

サービス・プロバイダ・ネットワーク・サーバ（104）は、ホーム・ネットワーク・オーソライザ（103）からのService_Specフィールド（705）をチェックし、要求されたサービスがサポートされない場合には、失敗を示すメッセージが、ホーム・ネットワーク・オーソライザ（103）に送られる。なお、失敗の原因を特定するために、あるエラー・コードを使用することも可能である。また、Service_Specフィールド（705）内の所定の属性が、サービス・プロバイダ・ネットワーク（1003）の現在の能力を超える場合には、サービス・プロバイダ・ネットワーク・サーバ（104）は、新しいセットの属性で、ホーム・ネットワーク・オーソライザ（103）とやり取りを行おうと試みることも可能である。これは、サービス・プロバイダ・ネットワーク・サーバ（104）によって提案された値に修正されたService_Specフィールド（705）を有する同一のService_Requestメッセージ（203）が、ホーム・ネットワーク・オーソライザ（103）に送り返されることによって達成される。

また、サービス・プロバイダ・ネットワーク・サーバ（104）は、

- Tunnel_Sepcフィールド（706）をチェックし、一致するトンネルのタイプを求める。複数の一致があるかもしれないが、サービス・プロバイダ・ネットワーク・サーバ（104）は最初に一致したものを選択すべきである。ネットワークに基づくトンネルのタイプに関しては、サービス・プロバイダ・ネットワーク・サーバ（104）は、返答メッセージ内にトンネルの終端点の情報を用意する必要がある。クライアントに基づくトンネルに関しては、サービス・プロバイダ・ネットワーク・サーバ（104）は、トンネルのタイプに固有の情報を用意し、返答情報にこの情報を含ませる。例えば、モバイルIP v6のタイプのスキームに関しては、サービス・プロバイダ・ネットワーク・サーバ（104）は、移動端末（101）にホーム・エージェントを割り当てる必要がある。また、返答メッセージ内に、あるセキュリティ情報を含ませることも可能である。なお、方向性の情報（例えば、一方向、両方向）もトンネル情報のフィールドに付加されてもよい。
- 15 サービス・プロバイダ・ネットワーク・サーバ（104）は、Service_Replyメッセージ（205）を用いて、ホーム・ネットワーク・オーソライザ（103）に対して返答を行う。Service_Replyメッセージ（205）には、図7に示されるようなService_Requestメッセージ（203）と同様の構造を使用することが可能である。
- 20 Home_Network_IDフィールド（701）、MT_IDフィールド（702）、及び、Session_IDフィールド（703）の内容は、対応するService_Requestメッセージ（203）から直接コピーされる。なお、これらのフィールドは、複数の端末のためにシグナリングのリンクが再利用される場合に、要求及び返答メッセージのペアを一致させるために、
- 25 ホームネットワークオーソライザ（103）によって使用される。

Service_Replyメッセージ（205）内のAddress_Requestフィールド

(704)の内容は、移動端末(101)に割り当てられたアドレスを含んでおり、それは、バイトでフィールドの長さを示す最初のオクテットを有するアドレスのエントリのリストであり得る。フィールドの次の部分はアドレスのリストであり、実際のアドレスを伴うアドレスのタイプを示す1オクテットを有している。ワイルドカードのアドレスも許可
5 されており、例えば、アドレス・フィールドがすべて0で満たされる場合には、WLANのローカルのメカニズム(例えばIPv6自動割り付け(非特許文献17)やDHCPを使用して、移動端末(101)がアドレスを形成することを示している。

10 また、Service_Replyメッセージ(205)内のService_Specフィールド(705)の内容には、サービス・プロバイダ・ネットワーク・サーバ(104)によって同意された属性が含まれている。すべての属性がサービス・プロバイダ・ネットワーク・サーバ(104)によって承認される場合には、対応するService_Requestメッセージ(203)内
15 のService_Specフィールド(705)と同一である。一方、同一でない場合には、サービス・プロバイダ・ネットワーク・サーバ(104)は、ホーム・ネットワーク・オーソライザ(103)に対して、対立した提案を行っていることになる。

また、Service_Replyメッセージ(205)内のTunnel_Specフィールド
20 ド(706)は、サービス・プロバイダ・ネットワーク・サーバ(104)によって選択されたトンネルの設定を含んでいる。このフィールドの正確な内容は、トンネルのタイプに依存しており、クライアントに基づくトンネル・タイプが選択された場合には、ただ1つのセッティングのみが必要となる。例えば、もしモバイルIPv6が同意されていれば、
25 このフィールドには、移動端末(101)に割り当てられたホーム・エージェントのアドレス及びバインディングアップデート認証のためのセ

セキュリティ・キーなどが含まれることとなる。また、Address_Request
フィールド（704）内のアドレスは、移動端末（101）のホーム・
アドレスとして使用される。また、ネットワークに基づくトンネルのタ
イプが選択される場合、このフィールドには、例えば、終端点アドレス
5 やトンネル識別子、サポートされるトンネルのタイプのそれぞれに関し
て必要となるすべての詳細な情報が含まれることとなる。

Service_Requestメッセージ（203）と並行して、ホーム・ネット
ワーク・オーソライザ（103）は、WLANサーバ（102）に対し
て、WLAN_Requestメッセージ（206）を送信する。このメッセージ
10 は、WLAN内のサービス提供に必要な設定の取り決めを行うためのも
のである。図8には、このメッセージの実施例が示される。

WLAN_Requestメッセージ（206）は、Service_Requestメッセー
ジ（203）のように、Home_Network_IDフィールド（801）及び
MT_IDフィールド（802）の2つのフィールドを含んでいる。
15 Home_Network_IDフィールド（801）は、加入者のホーム・ネット
ワークの識別子を含んでおり、あるネットワーク・ポリシーがサービス
提供に適用される場合に、WLANサーバ（102）に渡される。また、
MT_IDフィールド（802）は、移動端末（101）の位置を追跡する
ために使用される。例えば、移動端末（101）の下位レイヤの識別子
20 （例えば、MACアドレス）と関連するアクセス・ポイントの識別子
を利用することが可能である。

また、Address_Allocフィールド（803）は、移動端末（101）
にWLANのローカル・アドレスを割り当てる必要があるかどうかを示す
フラグと、使用されるべきアドレスのタイプである。ホーム・ネットワ
ーク・オーソライザ（103）は、選択されたトンネル・スキームに基
づいて、ローカル・アドレスが必要か否かを決定する。実際には、例え
25

ば、次の定義を用いて、このフィールドの最初のオクテットによって、アドレス割り付けが必要であるか否かが示される。

No_Allocation::=0x00;

Single_Stack_IPv4::=0x01;

5 Single_Stack_IPv6_FullAddress::=0x02;

Single_Stack_IPv6_Prefix::=0x03;

Dual_Stack_IPv4_Preferred::=0x04;

Dual_Stack_IPv6_Preferred_FullAddress::=0x05;

Dual_Stack_IPv6_Preferred_Prefix::=0x06

10 なお、このメッセージの実際の実施において、他の値が使用可能であることは、当業者にとっては明白である。

Service_Supportフィールド（804）は、WLAN内でサービス提供をサポートするために必要な属性をすべて含んでいる、複合したフィールドである。実際の内容は、サービスの特定であり、このフィールド
15 の内容の例は、データ構造1に説明されたものである。

また、Tunnel_Setupフィールド（805）も複合したフィールドであり、Service_Requestメッセージ（203）内のTunnel_Specフィールド（706）と同様のフォーマットが使用される。

また、WLAN_Requestメッセージ（206）の最後のフィールドは、
20 Security_Field（806）である。このフィールドは、メッセージ全体を完全に保護するために、セキュリティの関連付けが使用される。このフィールドの計算のために使用されるアルゴリズムは、実際の実施形態に依存している。

WLAN_Requestメッセージ（206）を受け取った後、WLANサーバ（102）は、WLANサービス・アドレス管理（207）を実行する。
25 例えば、ローカルのIPv6アドレスの割り付けが、ホーム・ネッ

トワーク・オーソライザ（１０３）によって要求された場合には、WLANサーバ（１０２）は、適切なネットワーク・セクションを見つけて、端末にIPv6アドレスを割り当てる。なお、必要ならば、さらにWLANサーバ（１０２）は、ゲートウェイの更新を行う（すなわち、WLANのファイア・ウォールに新しいアドレスの割り付けを行う）。これにより、移動端末（１０１）は、この割り当てられたローカル・アドレスを使用して、サービスにアクセスすることが可能となる。

WLANサーバ（１０２）は、さらにローカルの承認コントロールを実行するために、Service_Supportフィールド（８０４）内の情報を使用する。サービス・プロバイダ・ネットワーク・サーバ（１０４）と同様に、もし任意の属性がWLANの現在のキャパシティーを超える場合には、WLANサーバ（１０２）は、ホーム・ネットワーク・オーソライザ（１０３）との間で、例えば、ビット・レートの縮小やサービスの時間間隔の変更など、サービスの詳細に係る新しいセットの取り決めを試みる。

もし、クライアントに基づくトンネルのスキームが、ホーム・ネットワーク・オーソライザ（１０３）によって選択された場合には、WLANサーバ（１０２）は、特別な設定を行う必要がない。一方、ネットワークに基づくトンネル・スキームが使用される場合には、WLANサーバ（１０２）は、MT_IDフィールド（８０２）からの情報を用いて、トンネルの終端点を識別する必要がある。

WLANサーバ（１０２）は、WLAN_Replyメッセージ（２０８）を用いて、WLAN_Requestメッセージ（２０６）への返答を行う。

WLAN_Replyメッセージ（２０８）には、図８に示されるWLAN_Requestメッセージ（２０６）と同様の構造が利用される。Home_Network_IDフィールド（８０１）とMT_IDフィールド（８０２

）は、対応するWLAN_Requestメッセージ（206）から直接コピーされる。これらのフィールドは、要求及び返答メッセージのペアを一致させるために、ホーム・ネットワーク・オーソライザ（103）によって使用される。

- 5 また、WLAN_Replyメッセージ（208）内のAddress_Allocフィールド（803）には、移動端末（101）に割り当てられたWLANのローカル・アドレスの情報が含まれている。MT_Request_Aメッセージ（202A）内のAddress_Requestフィールド（307）に定義されるように、このフィールドの最初のオクテットは、アドレスのタイプを示している。このフィールドの次に続く部分には、移動端末（101）に
10 割り当てられる実際のアドレスが含まれており、例えば、IPv6アドレスが割り当てられる場合には、最初のオクテットは0x02となり、次の32オクテットには、実際のIPv6アドレスが含まれる。

- また、WLAN_Replyメッセージ（208）内のService_Supportフィールド（804）には、WLAN_Requestメッセージ（206）に定義されるサービスの属性の情報が含まれている。もし、WLANがこれらのサービスの属性を受け入れた場合には、WLANサーバ（102）は、WLAN_Requestメッセージ（206）から、それらを直接コピーする。一方、WLANサーバ（102）がその属性を受け入れることができなかった場合、WLAN_Replyメッセージ（208）内に新しい値をセット
15 した属性を加えて、新たな提案を送信する。

- また、WLAN_Replyメッセージ（208）内のTunnel_Setupフィールド（805）は、移動端末（101）へのトンネルの情報である。ここには、最初のオクテット内で使用されるトンネルのタイプ、及び、次のオクテットでトンネルのタイプに固有のデータが示されている。例
25 えば、モバイルIPv6がデータ・トラフィックに対して使用される場合

には、このフィールド内にはトンネルのタイプのみが存在し、
Address_Allocフィールド（８０３）のアドレスが移動端末（１０１）
の気付アドレスとして使用される。一方、モバイルＩＰｖ４が使用され
る場合には、このフィールドには、最初のオクテットにトンネルのタイ
5 プが含まれ、移動端末（１０１）に割り当てられるフォーリン・エー
ジェントのアドレスが後続する。

Service_Replyメッセージ（２０５）及びWLAN_Replyメッセージ（
２０８）の受信後、ホーム・ネットワーク・オーソライザ（１０３）は、
WLANサーバ（１０２）及びサービス・プロバイダ・ネットワーク・
10 サーバ（１０４）からの情報を統合する。もし、Service_Specフィール
ド（７０５）又はService_Supportフィールド（７０６）が、
Service_Requestメッセージ（２０３）又はWLAN_Requestメッセージ
（２０６）内のものとは異なっている属性の値を含んでいる場合には、
サービスの詳細を再度取り決める必要がある。このとき、ホーム・ネッ
15 トワーク・オーソライザ（１０３）は、サービス・プロバイダ・ネッ
トワーク・サーバ（１０４）又はWLANサーバ（１０２）によって提案
された新しい値をチェックし、もし、これらの新しい値を受け入れるこ
とが可能ならば、SPN_Configメッセージ（２１０）及びWLAN_Config
メッセージ（２１１）を用いて、新しい設定の承認を行う。

20 Service_Requestメッセージ（２０３）、Service_Replyメッセージ（
２０５）とWLAN_Requestメッセージ（２０６）、WLAN_Reply
message（２０８）とのメッセージのペアは、時間的な相関性を有して
いない。すなわち、それらは並行に行われるか、ホーム・ネットワーク
・オーソライザ（１０３）の実施にそれぞれ依存して１つずつ行われる。
25 例えば、WLANサーバ（１０２）との接続がアイドル状態ならば、ホ
ーム・ネットワーク・オーソライザ（１０３）は、Service_Requestメ

ッセージ（２０３）の代わりにWLAN_Requestメッセージ（２０６）を送送する決定を行うことが可能である。

また、再度やり取りが必要な場合に、新しいサービス・パラメータを確認するために、ホーム・ネットワーク・オーソライザ（１０３）から
5 サービス・プロバイダ・ネットワーク・サーバ（１０４）に対して、
SPN_Configメッセージ（２１０）が送られる。なお、SPN_Configメッセージ（２１０）には、Service_Requestメッセージ（２０３）と同一のメッセージ・フォーマットが使用される。また、もし同一のメッセージ・フォーマットを使用しない場合には、例えば、Address_Requestな
10 どのいくつかのフィールドが省略されることがある。

また、必要に応じて、トンネリングの情報が付加されてもよい。例えば、クライアントに基づくトンネル（例えば、モバイルIP）が使用される場合には、WLANサーバ（１０２）によって割り当てられる移動
端末（１０１）の気付アドレスが、Tunnel_Requestフィールド（３０
15 ８）に挿入される。また、ネットワークに基づくトンネルが使用される場合には、WLANのトンネルの終端点アドレスやポート番号などが、このメッセージで転送される。

また、WLAN_Configメッセージ（２１１）は、同様の目的で利用されるものであり、ホーム・ネットワーク・オーソライザ（１０３）は、
20 必要に応じて、このメッセージを使用して、WLANサーバ（１０２）に新しい設定を確認してもらう。また、さらに、この情報は、トンネルの情報を転送するために用いられることも可能である。例えば、ネットワークに基づくトンネルが使用される場合には、サービス・プロバイダ・ネットワーク（１００３）のトンネルの終端点アドレスやポート番号
25 などが、このメッセージでWLANサーバ（１０２）に転送され、その後、WLANサーバ（１０２）は、コレスポンデント・ノードに対して、

トンネルをセット・アップするよう命ずる。一方、クライアントに基づくトンネルが使用される場合には、端末のアドレスがこのメッセージに含まれ、その結果、WLANはデータ・トラフィックのためにファイア・ウォールを開くことが可能となる。

- 5 なお、サービス・セッションが終わったときに、移動端末（101）に割り当てられたリソースを無効にするために、ホーム・ネットワーク・オーソライザ（103）によって、これらの2つのメッセージ、SPN_Configメッセージ（210）及びWLAN_Configメッセージ（211）が使用可能であることは、当業者にとっては明白である。例えば、
- 10 移動端末（101）がもはやWLAN内に存在しないことを、ホーム・ネットワーク・オーソライザ（103）が検知した場合には、それは、すべて0にセットされたService_Supportフィールド（804）を含むWLAN_Configメッセージ（211）を出すことができる。WLANサーバ（102）は、この種のメッセージを受け取った後、移動端末（1
- 15 01）に割り当てられたリソースをすべて解放し、他の適切な動作を実行する。

- ホーム・ネットワーク・オーソライザ（103）は、MT_Request_Bメッセージ（202B）に対する返答として、MT_Reply_Bメッセージ（212B）を送る。このメッセージは、アクセス・ポイント（105
- 20 ） 、又は、他の付随した装置によって、メッセージMT_Reply_Aメッセージ（212A）として、移動端末（101）に転送される。なお、MT_Reply_Aメッセージ（212A）及びMT_Reply_Bメッセージ（212B）は、同一の内容及びフォーマットを有している。ホーム・ネットワーク・オーソライザ（103）と移動端末（101）との間のネットワーク・エレメントは、これらのメッセージの内容にアクセスせず、
- 25 また、アクセス・ポイント（105）は、単にメッセージ全体を再カプ

セル化して、それを転送する。MT_Reply_Aメッセージ（2 1 2 A）又はMT_Reply Bメッセージ（2 1 2 B）は、移動端末（1 0 1）とホーム・ネットワーク・オーソライザ（1 0 3）との間で共有されるセキュリティの関連付けによって暗号化される。なお、MT_Reply_Aメッ
5 ジ（2 1 2 A）は、対応するMT_Request_Aメッセージ（2 0 2 A）への返答であり、アクセス・ポイント（1 0 5）は、転送すべき移動端末（1 0 1）を把握することが可能である。

また、WLANサーバ（1 0 2）がMT_Reply_B_message（2 1 2 B）のパス上にある場合には、そのメッセージにWLAN_Configメッ
10 ジ（2 1 1）を乗せて運ぶことが可能である。例えば、WLANサーバ（1 0 2）が、WLAN内のダイアメータを用いて、移動端末（1 0 1）にMT_Reply_Bメッセージ（2 1 2 B）を転送するAAAサーバである場合には、MT_Reply_Bメッセージ（2 1 2 B）は、ダイアメーターEAP-Answer AVPにカプセル化可能である。一方、同じメッ
15 ジ内の別のAVPにWLAN_Configメッセージ（2 1 1）がカプセル化されてもよい。また、他の転送プロトコルが利用される場合でも、同じようなスキームが使用可能であることは、当業者にとっては明白である。

また、MT_Reply_Aメッセージ（2 1 2 A）は、図3に示されるMT_Request_Aメッセージ（2 0 2 A）と同一の構造を有している。
20 Message_Typeフィールド（3 0 1）は、MT_Request_Aメッセージ（2 0 2 A）のものと同一のフォーマットを有しており、このメッセージが要求ではなく、返答であることを示すための整数が使用される。また、Message_Lengthフィールド（3 0 2）は、Message_Typeフィールド（3 0 1）を含むメッセージの長さの合計を示すものである。また、
25 MT_Reply_Aメッセージ（2 1 2 A）内のDomain_Nameフィールド（3 0 3）及びMT_IDフィールド（3 0 4）は、MT_Request_Aメッセー

ジ（202A）内のものと同一である。なお、シグナリングを最適化するため、実際には、これらのフィールドが省略可能であることは、当業者にとっては明白である。

また、MT_Reply_Aメッセージ（212A）内のService_Requestフィールド（305）は、ユーザの加入情報に基づいて、ホーム・ネットワーク・オーソライザ（103）によってセットされるサービス特定情報を含むように使用される。例えば、もしユーザがIMSサービスを要求した場合には、P-CSCFアドレスが利用可能である。なお、このフィールドが、サービスの提供に必要な他の情報を含んでもよいことは、
5
10 当業者にとっては明白である。また、このフィールドの正確なフォーマットは、サービスに依存している。

また、MT_Reply_Aメッセージ（212A）内のSession_IDフィールド（306）は、MT_Request_Aメッセージ（202A）から直接コピーされるが、移動端末（101）によって要求されない場合、実際には
15 それを省略することが可能である。

また、MT_Reply_Aメッセージ（212A）内のAddress_Requestフィールド（307）は、移動端末（101）に割り当てられるアドレスを含んでいる。これは、ソース・アドレスとしてサービス・アプリケーションによって使用されるべきものである。このフィールドの最初のオクテットはアドレスのタイプであり、実際のアドレスが後続する。例えば、もしIPv6アドレスのプリフィックスが割り当てられれば、最初のオクテットは0x03となる。また、次の32オクテットは、実際のIPv6
20 アドレスを形成するために移動端末（101）によって使用されるプリフィックス情報を含んでおり、例えば、WLANゲートウェイアドレス、
25 DNSサーバアドレスなどの他のアドレス情報を含むことも可能である。これらの属性は、上記のアドレス情報に後続する。また、すべて0であ

るワイルドカードの値は、移動端末（１０１）が、実際のアドレス情報
を得るために、ローカルのステートレス（Stateless）のメカニズムを使
用すべきであることを示している。

また、MT_Reply_Aメッセージ（２１２Ａ）内のTunnel_Requestフ
5 ィールド（３０８）は、移動端末（１０１）によって要求されるサービ
スにアクセスするためのトンネリングの設定を含むものである。これは、
トンネルのタイプに依存し、このフィールドの最初のオクテットは、使
用されるトンネルのタイプを示している。

例えば、クライアントに基づくトンネルのタイプにモバイルＩＰｖ６
10 が使用される場合には、MT_Request_Aメッセージ（２０２Ａ）でトン
ネルのタイプが定義されるように、その値は0x06となる。タイプの属性
に続いて、WLANによって割り当てられる気付アドレス及びホーム・
エージェントのアドレス、そして、必要であればセキュリティ・キーが
存在する。Address_Requestフィールド（３０７）内のアドレスは、端
15 末に割り当てられたホーム・アドレスとなる。

また、ネットワークに基づくトンネルのタイプが使用された場合には、
タイプ属性に続いて、トンネルのローカルの終端点アドレスと、移動端
末（１０１）が安全に終端点と通信を行うためのセキュリティ・キーと
が存在する。

20 MT_Reply_Aメッセージ（２１２Ａ）内のWLAN_IDフィールド（３
０９）は、MT_Request_Aメッセージ（２０２Ａ）から直接コピーされ
る。なお、シグナリングを最適化するため、実際には、それを省略する
ことが可能である。

また、MT_Reply_Aメッセージ（２１２Ａ）のSecurity_Field（３１
25 ０）は、メッセージ全体を完全に保護するために使用され、移動端末（
１０１）とホーム・ネットワーク・オーソライザ（１０３）との間のセ

キュリティの関連付けが使用される。なお、ここでは、MT_Request_A
メッセージ（202A）のものと同一のアルゴリズムを使用すべきであ
る。

MT_Reply_Aメッセージ（212A）を受け取った後、移動端末（1
5 01）はすべての必要な情報を検索して、それに従って構成を行い、こ
の設定を使用して、実際のサービス・セッション（213）を開始する
ことが可能となる。

実際には、移動端末（101）は、例えば、ビデオストリーミング・
セッションと一緒にVoice-over-IPセッションを行うなど、いくつかのサ
10 ービスを同時に要求することが可能である。すなわち、シグナリング内
に、異なるサービス・プロバイダ・ネットワークを関係付けることが可
能である。同一のメッセージ内にいくつかのサービスの要求をまとめる
シナリオにおいて、上記と同一のメカニズム及びメッセージの構造を使
用することが可能である。例えば、MT_Request_Aメッセージ（202
15 A）内に、Service_Requestフィールド（305）、Session_IDフィー
ルド（306）、Address_Requestフィールド（307）、Tunnel_Request
フィールド（308）の複数のセットを存在させることが可能である。
これらの4つのフィールドはグループ化され、移動端末（101）によ
って要求された各サービスは、これらの4つのフィールドの1グループ
20 を含んでいる。例えば、MT_Request_Aメッセージ（202A）が
Voice-over-IPセッション及びビデオストリーミング・セッションを要求
した場合には、列挙された4つのフィールドのグループが2つ存在する。

MT_Request_Aメッセージ（202A）と同じ内容を含んでいる
MT_Request_Bメッセージ（202B）を受け取った後、ホーム・ネッ
25 トワーク・オーソライザ（103）は、移動端末（101）によって要
求される1つの特定のサービスに対応した、これらの4つのフィールド

の各セットから情報を検索する。ホーム・ネットワーク・オーソライザ
(103)は、単一のサービスの要求に対して、上記のように要求され
たサービスの各々のためのシグナリングを実行する。例えば、ホーム・
ネットワーク・オーソライザ(103)は、IMSサブシステム及びス
5 トリーミング・サービスを提供するネットワークの両方に、
Service_Requestメッセージ(203)を送る。また、異なる各サービ
スに係るWLAN_Requestメッセージ(206)が、同一のWLANに送
られる。ホーム・ネットワーク・オーソライザ(103)は情報を集め、
ただ1つのメッセージを送ることが可能である。同一のWLANに多数
10 のWLAN_Requestメッセージ(206)を送る必要がある場合には、そ
れらのうちの1つだけが、ローカルのアドレスの割り付けの要求を行う
必要がある。

ホーム・ネットワーク・オーソライザ(103)は要求されたサービ
スの順序に従って、1つのMT_Reply_Bメッセージ(212B)にすべ
15 てのサービス情報を統合し、アクセス・ポイント(105)を介して、
移動端末(101)に転送する。その後、移動端末(101)は統合さ
れたMT_Reply_Aメッセージ(212A)内の情報を用いて、それ自体
のアドレス構成を行うことが可能となる。

なお、移動端末(101)が並行して多数のサービスを要求した場合
20 には、異なるサービス・プロバイダ・ネットワークからその端末に異な
るアドレスが割り当てられる可能性があり、さらに、異なるサービス・
セッションにおいて異なるトンネルが設定される可能性がある。このシ
ナリオでは、特別な中間層プロセッサ(mid-layer processor)が必要と
なる。Session_IDフィールド(306)で使用されるようなサービス・
25 セッション識別子が、中間層プロセッサによって使用されて、アドレス
及びトンネルの設定が多重化される。

移動端末（１０１）内の中間層プロセッサは、異なるサービス・セッションにおけるアドレス及びトンネル情報のローカルのデータベースを保持している。サービス・セッションが移動端末（１０１）で生成された場合、中間層プロセッサはそのための識別子を作成する。これは、

- 5 MT_Request_Aメッセージ（２０２Ａ）のSession_IDフィールド（３０６）内で使用されるセッション識別子である。アドレス及びトンネル情報をすべて含むMT_Reply_Aメッセージ（２１２Ａ）を受け取った後、中間層プロセッサは、セッション識別子によって指標化（インデックス化）されたすべての情報を含むデータベース内に、新しいエントリを作成する。サービス・アプリケーションが、新しい接続セッションを開始する必要がある場合には、中間層プロセッサに対してセッション識別子が設定されたリクエストを送り、中間層プロセッサは、このセッション識別子を用いて、データベースから、対応するアドレス及びトンネル情報を検索する。アドレス及びトンネル情報は、例えば、ＩＰレイヤなどの通常
- 10 の通常のスタックによって使用され、接続を行うために、ソケットなどの適切なバインディングが作られる。

- 20 なお、実際には、例えば、ＷＬＡＮサーバ（１０２）などのようなコントローラのないＷＬＡＮが存在可能であることは、当業者にとっては明白である。このような場合には、移動端末（１０１）はアドレスの割り付け及びトンネルの設定のために、ＷＬＡＮのローカルのメカニズムを使用しなくてはならない。ホーム・ネットワーク・オーソライザ（１０３）は、MT_Reply_Aメッセージ（２１２Ａ）内のAddress_Requestフィールド（３０７）及びTunnel_Requestフィールド（３０８）をすべて０にセットし、これによって、移動端末（１０１）に対して、例えば、
- 25 DHCPv6、MIPv6などのＷＬＡＮメカニズムを使用してアドレス構成を行うよう強いることになる。

また、ある場合では、移動端末（１０１）が、WLAN内のサービス登録の取り消しを望むことがある。サービスの登録抹消を行う場合でも上記のメカニズムを使用することが可能であることは、当業者にとっては明白である。移動端末（１０１）は、サービスの終了を示す特別の値
5 がService_Requestフィールド（３０５）に設定されたMT_Request_Aメッセージ（２０２Ａ）を送出することが可能である。例えば、Service_Requestフィールド（３０５）は「terminate.request.IMS.foo.bar.operator-name.operatorgroup.gprs」のような値を含むことが可能である。なお、「request（要求）」キーワードの前の「terminate（終了）」が
10、「request（要求）」キーワードの後に付けられているAPNによって示されたサービスを終了するためのフラグである。また、MT_Request_Aメッセージ（２０２Ａ）のSession_IDフィールド（３０６）は、終了するサービスのセッション識別子に設定可能であり、このタイプのMT_Request_Aメッセージ（２０２Ａ）では、Address_Requestフィールド
15（３０７）及びTunnel_Requestフィールド（３０８）を省略することが可能である。

ホーム・ネットワーク・オーソライザ（１０３）は、通常と同様に、MT_Request_Aメッセージ（２０２Ａ）の処理を行い、そのService_Requestフィールド（３０５）内に「終了」のキーワードを見
20つけた場合には、Session_IDフィールド（３０６）からサービス・セッション識別子を取り出す。そして、ホーム・ネットワーク・オーソライザ（１０３）は、サービス登録時に作られたセッション・エントリを探すため、そのデータベースを探索する。このセッション・エントリは、例えば、割り当てられたアドレス、トンネル設定などのサービスの設定
25に関する情報を格納している。この情報を用いて、通常と同様に、ホーム・ネットワーク・オーソライザ（１０３）は、サービス・プロバイダ

・ネットワーク・サーバ（１０４）にService_Requestメッセージ（２０３）を送り、WLANサーバ（１０２）にWLAN_Requestメッセージ（２０６）を送る。これらのメッセージにおいて、Service_Specフィールド（７０５）及びService_Supportフィールド（８０４）は、すべて
5 0にセットされる。

サービス・プロバイダ・ネットワーク・サーバ（１０４）とWLANサーバ（１０２）は、通常通り、メッセージを処理し、Service_Specフィールド（７０５）及びService_Supportフィールド（８０４）がすべて0に設定されているのを読んで、サービス終了の要求であることを把握する。これらの２つのサーバは、サービス登録時に作られたサービス・セッション・エントリを探すため、それらのデータベースを検索し、例えば、IPアドレスや予約している帯域幅などのサービス・セッションに対応するリソースを解放する。

ホーム・ネットワーク・オーソライザ（１０３）が、サービス・プロバイダ・ネットワーク（１００３）及びWLANから通知を受け取った後、MT_Reply_Aメッセージ（２１２Ａ）が、移動端末（１０１）に返される。このメッセージは、サービスを終了し、予約されていたリソースが解放されたことを通知するものである。このMT_Reply_Aメッセージ（２１２Ａ）では、Service_Requestフィールド（３０５）に、その
15 結果に関する情報が含まれている。例えば、このフィールドにおいて、次の値「removed.request.IMS.foo.bar.operator-name.operator-group.gprs」を使用することが可能である。ここでは、「request」キーワードの前の「removed」キーワードが、サービスの登録抹消の成功を示している。なお、例えば、「removed」キーワードの後に情報を付加するなど、特別な情報を含めてもよいことは、当業者にとっては明白である。
20

また、移動端末（１０１）へのサービス提供の過程において、ポリシ

ー・コントロールを含ませることも可能である。例えば、GPRSインターフェースを使用する端末は、149Kbpsのアクセス・レートが与えられている。この端末がWLANに入った場合、その端末は、同じサービスにアクセスするためにWLANインターフェースを使用するよう移行する。WLANは、はるかに高いエア・インターフェース帯域幅を提供するので、端末がより高いアクセス・レート（例えば、1Mbps）を享受することを切望する。移動端末（101）に対して、このより高いサービス・レートを与えるためには、ポリシー・コントロール・フレームワークが起動され、例えば、ゲートウェイ・フィルタなど、対応するポリシー設定を修正する必要がある。上記の例では、例えば、GGSNなどの制御点が、GPRSインターフェースを使用してサービスを始める場合には、GGSNは、端末のサービスのために149Kbpsの帯域幅のみを予約すればよい。また、移動端末（101）が、再びWLANサービスを利用して、サービス・セッションを登録する場合、ポリシー・サーバは、GGSNの設定を1Mbpsに修正すべきである。なお、他の種類の設定やコントロール・ノードがポリシー・コントロールに含まれることは、当業者にとっては明白である。

この種のポリシー・コントロールは、ユーザの加入情報に従って行われるべきであり、したがって、ホーム・ネットワーク・ドメイン内で行われるべきである。本発明は、サービスの要求及びアドレス（トンネルの設定）を扱うためにホーム・ネットワーク・オーソライザ（103）を使用するものである。したがって、それは、ポリシー・コントロール決定のために必要な情報をすべて有しており、ホーム・ネットワーク・ドメインのポリシー・サーバにホーム・ネットワーク・オーソライザ（103）から、こうした情報を渡すことが可能である。ポリシー・サーバは、このとき、例えば、GGSNなどのコレスポンディング・ノード

を適宜動作させるよう操作可能とするポリシー・コントロール・インターフェースを利用することが可能である。さらに、ポリシー・サーバは、ポリシー・コントロール・フレームワークを使ったサービス提供に関連する他のネットワークに通知を行うことも可能であり、例えば、ホーム・ネットワーク・ドメインのポリシー・サーバは、WLAN内のポリシー・サーバに対して、新しいアクセス・レートの制限を通知することが可能であり、その結果、WLANポリシー・サーバは、ローカルの承認管理機構を適宜調節することが可能となる。

また、図9は、ホーム・ネットワーク・オーソライザ（103）とポリシー・サーバとの間で使用されるメッセージの実施例を示すものである。このメッセージは、Operationフィールド（901）から始まる。このフィールドは、ポリシー・サーバによって行われる動作を示すものであり、可能な値は次の通りである。

Install::=0x01

15 Remove::=0x02

Update::=0x03

ホーム・ネットワーク・オーソライザ（103）が移動端末（101）から新しいサービス・セッションの要求を受け取った場合、Operationフィールド（901）内に「Install」の値を使用する。また、移動端末（101）がサービス・セッションを終了する場合には、ホーム・ネットワーク・オーソライザ（103）は、Operationフィールド（901）内に「Removed」の値を使用する。また、移動端末（101）からのサービスの要求がアクティブなサービス・セッションを参照している場合には、「Update」の値を使用する。なお、実際の実施においては、他のタイプの値の使用が可能であることは、当業者にとっては明白である。

また、2番目のフィールドは、MT_IDフィールド（902）である。

このフィールドは、移動端末（101）の識別子を含んでおり、例えば、モバイルのユーザのIMSIが使用可能である。

また、3番目のフィールドは、MT_Locationフィールド（903）である。このフィールドは、例えば、端末が所定のWLANに存在する場合
5 合には、2倍のアクセス・レートを提供するなど、位置に基づくサービスのポリシーを検索するために、ポリシー・サーバによって使用されるものである。このフィールドは、例えば、MT_Request_Aメッセージ（202A）のWLAN_IDフィールド（309）からのWLAN識別子を含むものである。

10 また、次のフィールドは、MT_Serviceフィールド（904）である。このフィールドは、移動端末（101）によって、どのような種類のサービスがアクセスされているかを示すものである。さらに、このフィールドが、サービス・セッション情報を含むことも可能である。このフィールドの内容の例としては、APNにセッション識別子を加えたものが
15 可能である。

また、次のフィールドは、Tunnel_Settingフィールド（905）である。このフィールドは、WLAN内で移動端末（101）によって使用されるトンネルの設定を示すものである。このフィールドの内容はトンネルのタイプであり、トンネルの終端点アドレス、ポート番号などが後
20 続する。なお、正確なフォーマットは、トンネルのタイプに依存する。また、使用されるトンネルのタイプは、MT_Request_Aメッセージ（202A）のTunnel_Requestフィールド（308）で定義されたものである。

また、メッセージの最後のフィールドは、MT_Addressフィールド（
25 906）である。このフィールドは、WLAN内で移動端末（101）によって使用されるアドレスを含むものである。これは、ポリシー・サ

サーバによって使用され、サービスにアクセスするフィルタリングの規則を設定することが可能となる。

なお、実際には、メッセージ・フィールドが上記ほど正確な順序で並べられる必要がないことは、当業者にとっては明白である。また、各フィールドは、さらに、本実施例に記述されない他の情報を含むことが可能である。

産業上の利用可能性

本発明は、WLAN相互接続において、端末のアドレス割り当てを管理する管理方法を提供する。本発明の適用によって、移動端末には、それが要求したサービスとその加入情報に基づいてアドレスの割り当てが行われ、ローカル・リソースへのアクセスを必要とせずに、アドレス管理が実行可能となる。さらに、本発明は、WLAN相互接続におけるトンネルの設定のコントロール方法を提供する。ここでは、移動端末は、サービス許可と同時にネットワーク及びクライアントに基づくトンネルの設定をサポートすることができる。さらに、本発明は、ポリシー・コントロール・フレームワークでの相互接続の方法を提供する。提供されるインターフェースを用いることによって、サービス許可、アドレス割り当て、及び、トンネル設定情報をポリシー・サーバに伝播することが可能となり、よりよく端末にサービスを配信するために適切な動作を行うことが可能となる。すべての方法において、端末とそのホーム・ドメイン・サーバとの1回の往復メッセージの交換で、アドレス管理、トンネルの設定及びサービスの許可を達成することが可能である。したがって、貴重なシグナリングの時間や帯域幅が節約される。

請 求 の 範 囲

1. 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをアドレスの管理のために利用することによって、前記コントローラがサービス許可情報に基づくアドレス割り当ての管理を行うことが可能であり、ローカルWLANアクセス制御に基づくことなく、WLAN相互接続において前記移動端末のアドレス割り当ての管理を行うためのシステム。
- 5 10
2. 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをトンネルの管理のために利用することによって、前記コントローラがサービス許可情報に基づくトンネル管理を行うことが可能であり、ローカルWLANアクセス制御に基づくことなく、WLAN相互接続において前記移動端末のトンネルの管理を行うためのシステム。
- 15
3. 移動端末と、前記移動端末のユーザ加入情報にアクセス可能であり、前記移動端末のホーム・ドメイン内に配置されているコントローラとの間におけるセキュリティ保護された終端点間サービス許可シグナリングをアドレス及びトンネルの管理のために利用することによって、前記コントローラがサービス許可情報に基づくアドレス割り当て及びトンネルの管理を行うことが可能であり、ローカルWLANアクセス制御に基づくことなく、WLAN相互接続において前記移動端末のアドレス
- 20 25

割り当て及びトンネルの管理を行うためのシステム。

4. 前記ローカルWLANアクセス制御処理に由来したシグナリング・メッセージの保護及び暗号化のためのセキュリティ連携を利用することによって、前記WLAN相互接続の前記シグナリング・メッセージを保護するよう構成されている請求項1から3のいずれか1つに記載のシステム。

5. 前記移動端末のドメイン情報を利用することによって、前記移動端末のホーム・ドメイン内の前記コントローラの位置情報を特定するよう構成されている請求項1から3のいずれか1つに記載のシステム。

6. 前記移動端末がそのドメイン情報をメッセージ内に埋め込み、前記移動端末と前記コントローラとの間に存在する中間ノードが前記ドメイン情報を参照して、前記ドメイン情報に基づいて前記メッセージを転送することによって、前記中間ノードが、前記コントローラに前記メッセージを転送するためのアドレスを決定するよう構成されている請求項1から3のいずれか1つに記載のシステム。

7. i. アドレス割り当て要求及びアドレス割り当て応答に、所定のワイルドカード値を使用することによって、前記移動端末におけるステートレスなアドレス構成をサポートし、

ii. 前記アドレス割り当て要求及び前記アドレス割り当て応答に、アドレスのタイプのリストを入れることによって、前記移動端末におけるアドレスの異なるタイプをサポートし、

iii. アドレス管理情報にアドレスのプリフィックスを入れることに

よって、前記移動端末に対する複数のアドレスの割り当てをサポートするよう構成されている請求項 1 又は 3 に記載のシステム。

8. i. 前記移動端末が、前記サービス・アクセス・セッションを一意に識別する識別子を生成し、
- 5 ii. 前記移動端末と前記コントローラとの間のアドレスに係るメッセージに、前記サービス・アクセス・セッションの識別子を入れることによって、アドレス割り当て処理と前記サービス・アクセス・セッションとの関連付けを行い、
- 10 iii. 前記コントローラが、前記移動端末の前記サービス・アクセス・セッションで利用される前記アドレスをトレースし、
- iv. 前記コントローラが、前記サービス・アクセス・セッションの識別子を利用して、前記サービス・アクセス・セッションにおいて前記移動端末によって使用されるアドレスを検索するよう構成されている請求項 1 又は 3 に記載のシステム。
- 15

9. 前記コントローラが、前記サービス・アクセス・セッションで使用される前記移動端末のアドレスの格納管理を行うためのバックエンド・サーバを利用するよう構成されている請求項 8 に記載のシステム。
- 20

10. 前記コントローラは、
- i. 前記移動端末の識別子と前記サービス・アクセス・セッションの識別子とを指標とするエントリが前記コントローラのレコード内に存在しない場合には、前記移動端末の識別子と、前記サービス・アクセス
- 25 ・セッションの識別子とを指標とする新たなエントリを作成し、
- ii. 前記サービス・アクセス・セッション用に前記移動端末に割り

当てる前記アドレスが設定された前記エントリを格納し、

iii. 前記移動端末が前記サービス・アクセス・セッションを終了した場合には、格納されている前記エントリを削除して、

前記コントローラが、前記WLAN相互接続における前記移動端末の
5 前記アドレス構成を保持するよう構成されている請求項8に記載のシステム。

1 1. i. サービス許可メッセージにおいて、アドレス割り当て要求とそれに対応するサービス・アクセス要求とをグループ化することによって、複数の異なるサービス・アクセス・セッションに対する複数のアドレスの割り当てをサポートし、

ii. 前記コントローラが、前記移動端末の異なるサービス・アクセス要求に基づいて、異なるアドレス構成を取得して、

前記移動端末における同時サービス・セッションが可能となるよう構成されている請求項1又は3に記載のシステム。
15

1 2. i. 前記移動端末が、対応する前記アドレス構成と共に前記サービス・アクセス・セッション情報を格納するためのローカルデータベースを保持し、

20 ii. サービス・アクセス・セッションの識別子を使用して、アドレスを多重化することによって、前記移動端末が、異なるサービスにアクセスするために異なるアドレスを使用して、

複数のサービス・セッションに対する複数のアドレス構成をサポートするよう構成されている請求項11に記載のシステム。

25

1 3. i. 前記ポリシー・サーバとのインターフェースを設定

することによって、前記コントローラが、前記移動端末にサービスを提供するためのポリシー構成を修正できるようにし、

- ii. WLAN内の前記移動端末にサービスを提供するためのコントロール・ノードに対するポリシー・コントロール・フレームワークを通じたポリシー・シグナリングを、前記コントローラに開始させることによって、前記コントロール・ノードに関するポリシー設定を適応させて、
- ポリシー設定の調整が可能となるよう構成されている請求項1から3のいずれか1つに記載のシステム。

- 10 14. 前記サービスの許可を行うサービス・オーソライザと、前記ポリシー・サーバとの間の情報交換に利用されるメッセージのフォーマットが、

- i. 前記ポリシー・サーバで行われる動作を示すオペレーション識別子部と、
- 15 ii. 前記移動端末の識別子を含む移動端末識別子部と、
- iii. 前記移動端末に対して、前記移動端末の位置に基づくポリシーを適用するための前記移動端末の位置情報を含む移動端末位置情報部と、
- iv. 前記サービスのタイプと、必要に応じて前記サービスのセッション識別子とを含む移動端末サービス情報部と、
- 20 v. 前記サービスにアクセスするために、前記移動端末によって利用されるトンネル設定情報を含むトンネル設定情報部と、
- vi. 前記サービスにアクセスするための前記移動端末の前記アドレスを含むアドレス情報部とを、
- 有する請求項13に記載のシステム。

25

15. i. 移動端末のユーザ加入情報にアクセス可能であり、

前記移動端末のホーム・ドメイン内に配置されているコントローラに対して、前記移動端末が、セキュリティ保護された終端点間のサービス許可要求と共に、アドレス管理要求を送信するステップと、

- ii. 前記コントローラが、前記サービス許可要求及び前記ユーザ加入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うためのアドレスを割り当てるステップと、

iii. 前記コントローラが、セキュリティ保護された終端点間サービス許可シグナリングを用いて、アドレス管理情報を前記移動端末に送信するステップとを、

- 10 有し、ローカルWLANアクセス制御に基づくことなく、WLAN相互接続において前記移動端末が前記サービスにアクセスするためのアドレス割り当ての管理を行うための方法。

16. i. 移動端末のユーザ加入情報にアクセス可能であり、
15 前記移動端末のホーム・ドメイン内に配置されているコントローラに対して、前記移動端末が、セキュリティ保護された終端点間のサービス許可要求と共に、トンネル管理要求を送信するステップと、

- ii. 前記コントローラが、前記サービス許可要求及び前記ユーザ加入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うためのトンネル構成を決定するステップと、

iii. 前記コントローラが、セキュリティ保護された終端点間サービス許可シグナリングを用いて、前記トンネル構成情報を前記移動端末に送信するステップとを、

- 20 有し、ローカルWLANアクセス制御に基づくことなく、WLAN相互接続において前記移動端末が前記サービスにアクセスするためのトンネルの管理を行うための方法。

17. i. 移動端末のユーザ加入情報にアクセス可能であり、
前記移動端末のホーム・ドメイン内に配置されているコントローラに対
して、前記移動端末が、セキュリティ保護された終端点間のサービス許
可要求と共に、アドレス及びトンネル管理要求を送信するステップと、
5 ii. 前記コントローラが、前記サービス許可要求及び前記ユーザ加
入情報に基づいて、前記移動端末が前記サービスへのアクセスを行うた
めのアドレス及びトンネル構成を決定するステップと、
 iii. 前記コントローラが、セキュリティ保護された終端点間サービ
10 ス許可シグナリングを用いて、前記アドレス及び前記トンネル構成に係
る情報を前記移動端末に送信するステップとを、
有し、ローカルWLANアクセス制御に基づくことなく、WLAN相
互接続において前記移動端末が前記サービスにアクセスするためのアド
レス割り当て及びトンネルの管理を行うための方法。

15

18. 前記ローカルWLANアクセス制御処理に由来したシグナ
リング・メッセージの保護及び暗号化のためのセキュリティ連携を利用
することによって、前記WLAN相互接続の前記シグナリング・メッセ
ージを保護する請求項15から17のいずれか1つに記載の方法。

20

19. 前記移動端末のドメイン情報を利用することによって、前
記移動端末のホーム・ドメイン内の前記コントローラの位置情報を特定
する請求項15から17のいずれか1つに記載の方法。

25

20. 前記移動端末がそのドメイン情報をメッセージ内に埋め込
み、前記移動端末と前記コントローラとの間に存在する中間ノードが前

記ドメイン情報を参照して、前記ドメイン情報に基づいて前記メッセージを転送することによって、前記中間ノードが、前記コントローラに前記メッセージを転送するためのアドレスを決定する請求項 15 から 17 のいずれか 1 つに記載の方法。

5

21. 前記移動端末によって要求される前記サービスを提供するネットワーク内のアドレス管理エンティティと前記コントローラとの間で、前記移動端末による前記サービスへのアクセスに利用されるアドレスの交渉を行うステップをさらに有する請求項 15 に記載の方法。

10

22. i. 前記移動端末が、前記コントローラに対して送信するアドレス割り当て要求に、特定のアドレスを入れるステップと、

ii. 前記移動端末からの前記アドレス割り当て要求と、前記移動端末によりアクセスされるサービスに係る情報とに従って、使用される前

15 記アドレスを前記移動端末に割り当てるステップとを、

有し、前記移動端末におけるサービス中断を抑制する請求項 15 に記載の方法。

23. i. 前記移動端末が、前記トンネル要求メッセージに、

20 前記トンネルのタイプのリストを入れるステップと、

ii. 前記移動端末及びコントローラが、前記トンネル要求メッセージ及びトンネル構成メッセージに、トンネルの方向に係る情報を入れるステップとを、

25 有し、複数のトンネルのタイプ及び方向をサポートする請求項 16 又は 17 に記載の方法。

24. 前記移動端末によって要求される前記サービスを提供するネットワーク内の実際のトンネル終端点と前記コントローラとの間で、前記移動端末による前記サービスへのアクセスに利用されるトンネル構成の交渉を行うステップをさらに有し、前記移動端末の前記トンネル構成の管理を行う請求項16又は17に記載の方法。

25. i. 前記コントローラが、前記移動端末による前記サービスへのアクセスに利用されるトンネルを管理する前記WLAN内のトンネル管理エンティティと通信を行うステップと、
- 10 ii. 前記WLAN内の前記トンネル管理エンティティが、前記コントローラとの通信結果に応じて、前記トンネルを使用可又は使用不可とするステップとを、

さらに有し、前記移動端末の前記トンネル構成の管理を行う請求項16又は17に記載の方法。

15

26. 前記コントローラが、前記WLAN内の前記トンネル終端点の識別及び構成を行うために、前記WLAN内のトンネル管理エンティティと通信を行うステップと、

- 前記コントローラが、前記移動端末に前記サービスを提供するネットワーク内の前記トンネル終端点の識別及び構成を行うために、前記ネットワーク内のトンネル管理エンティティと通信を行うステップとを、
- 20

さらに有し、前記移動端末が前記サービスにアクセスするためのサイト間ネットワーク・トンネルの設定を行う請求項16又は17に記載の方法。

25

27. 前記コントローラが、前記ユーザ加入情報を参照するため、

前記移動端末のホーム・ネットワーク内のバックエンド・サーバとの通信を行うステップを有する請求項 16 又は 17 に記載の方法。

28. 前記移動端末によって使用されるメッセージのフォーマットが、
- 5 i. すべてのネットワーク・ノードがアクセス可能な前記移動端末のホーム・ドメイン情報部と、
- ii. 前記サービス要求を許可するノードのみがアクセス可能な前記ユーザの識別情報部と、
- 10 iii. 前記サービス要求を許可するノードのみがアクセス可能な 1 つ以上のサービス許可要求を含むサービス要求情報部と、
- iv. WLAN 識別情報部と、
- v. 前記サービス要求に対応する 1 つ以上のアドレス要求を含むアドレス要求情報部とを、
- 15 有する請求項 15 又は 17 に記載の方法。

29. 前記移動端末によって使用されるメッセージのフォーマットが、
- i. 前記移動端末のホーム・ドメインの識別情報部と、
- 20 ii. 前記サービス要求を許可するノードのみがアクセス可能な前記ユーザの識別情報部と、
- iii. 前記サービス要求を許可するノードのみがアクセス可能な 1 つ以上のサービス許可要求を含むサービス要求情報部と、
- iv. WLAN の識別子を含む WLAN 識別情報部と、
- 25 v. 前記サービス要求に対応する 1 つ以上のトンネル構成要求を含むトンネル構成要求情報部とを、

有する請求項 1 6 又は 1 7 に記載の方法。

3 0. 前記コントローラによって使用されるメッセージのフォーマットが、

- 5 i. 前記移動端末のホーム・ネットワークの識別情報部と、
 - ii. 前記サービスの要求に関するサービス・セッションの識別情報部と、
 - iii. 前記サービス要求における前記移動端末の識別情報部と、
 - iv. 1 つ以上のサービス要求を含むサービス要求情報部と、
 - 10 v. 前記サービス要求に対応する 1 つ以上のアドレス構成要求を含むアドレス構成要求情報部とを、
- 有する請求項 2 1 に記載の方法。

3 1. 前記コントローラによって使用されるメッセージのフォーマットが、

- 15 i. 前記移動端末のホーム・ネットワークの識別情報部と、
 - ii. 前記サービスの要求に関するサービス・セッションの識別情報部と、
 - iii. 前記サービス要求における前記移動端末の識別情報部と、
 - 20 iv. 1 つ以上のサービス要求を含むサービス要求情報部と、
 - v. 前記サービス要求に対応する 1 つ以上のトンネル構成要求を含むトンネル構成要求情報部とを、
- 有する請求項 2 4 に記載の方法。

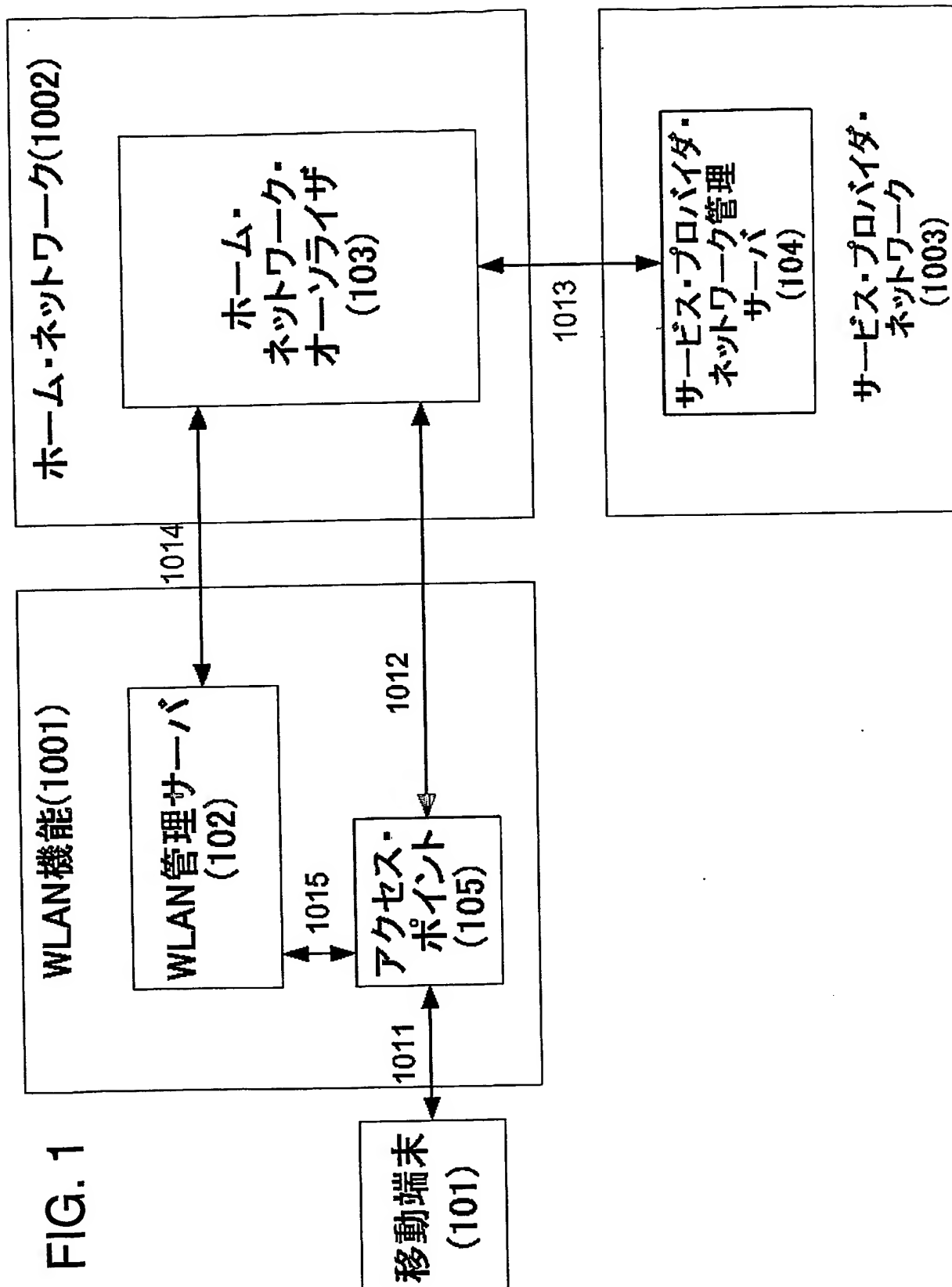


FIG. 2

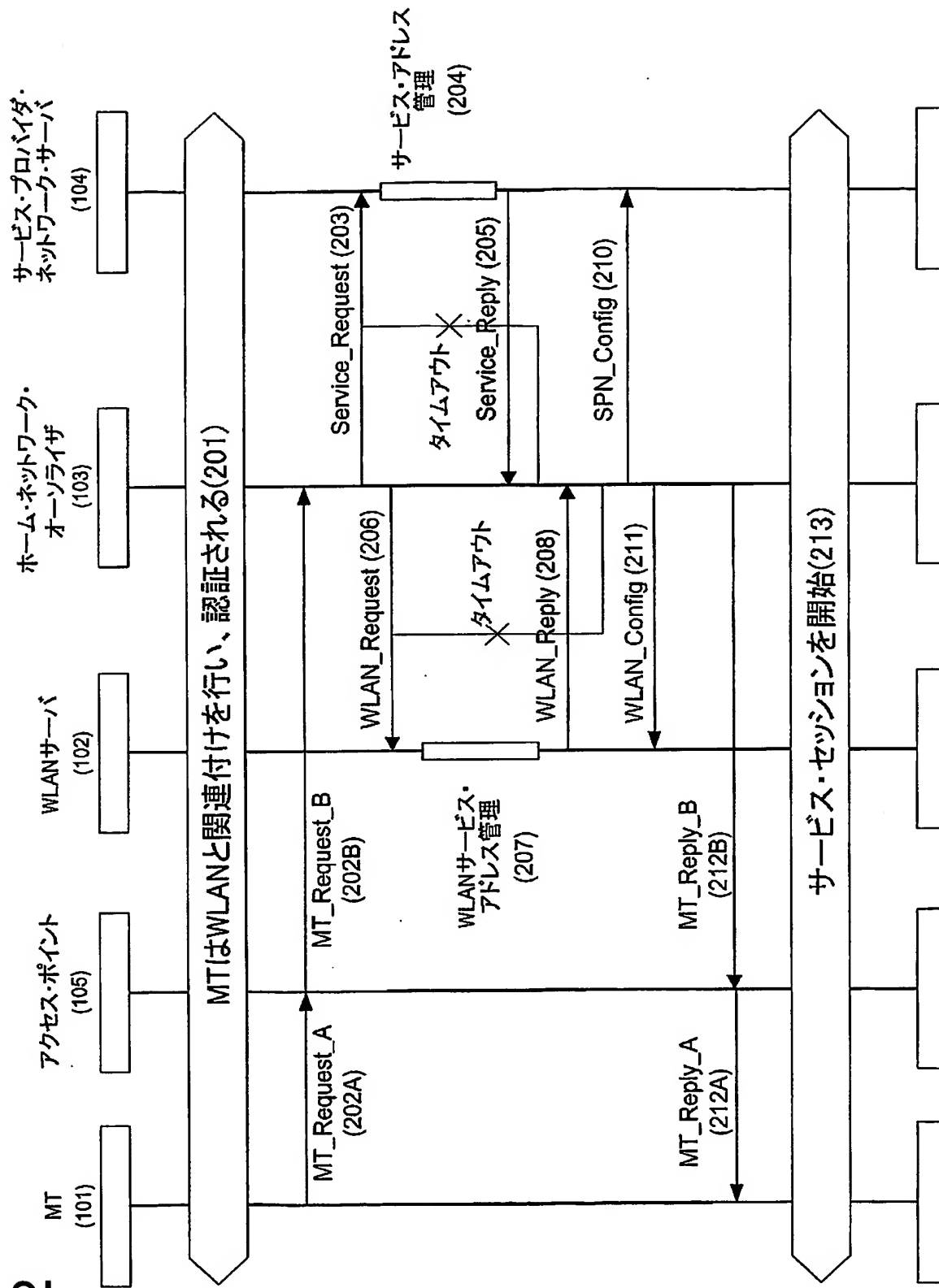


FIG. 3

Message_Type (301)
Message_Length (302)
Domain_Name (303)
MT_ID (304)
Service_Request (305)
Session_ID (306)
Address_Request (307)
Tunnel_Request (308)
WLAN_ID (309)
Security_Field (310)

FIG. 4

Address_Type (401)
Suggestion_Length (402)
Address_Suggestions (403)

Fig. 5

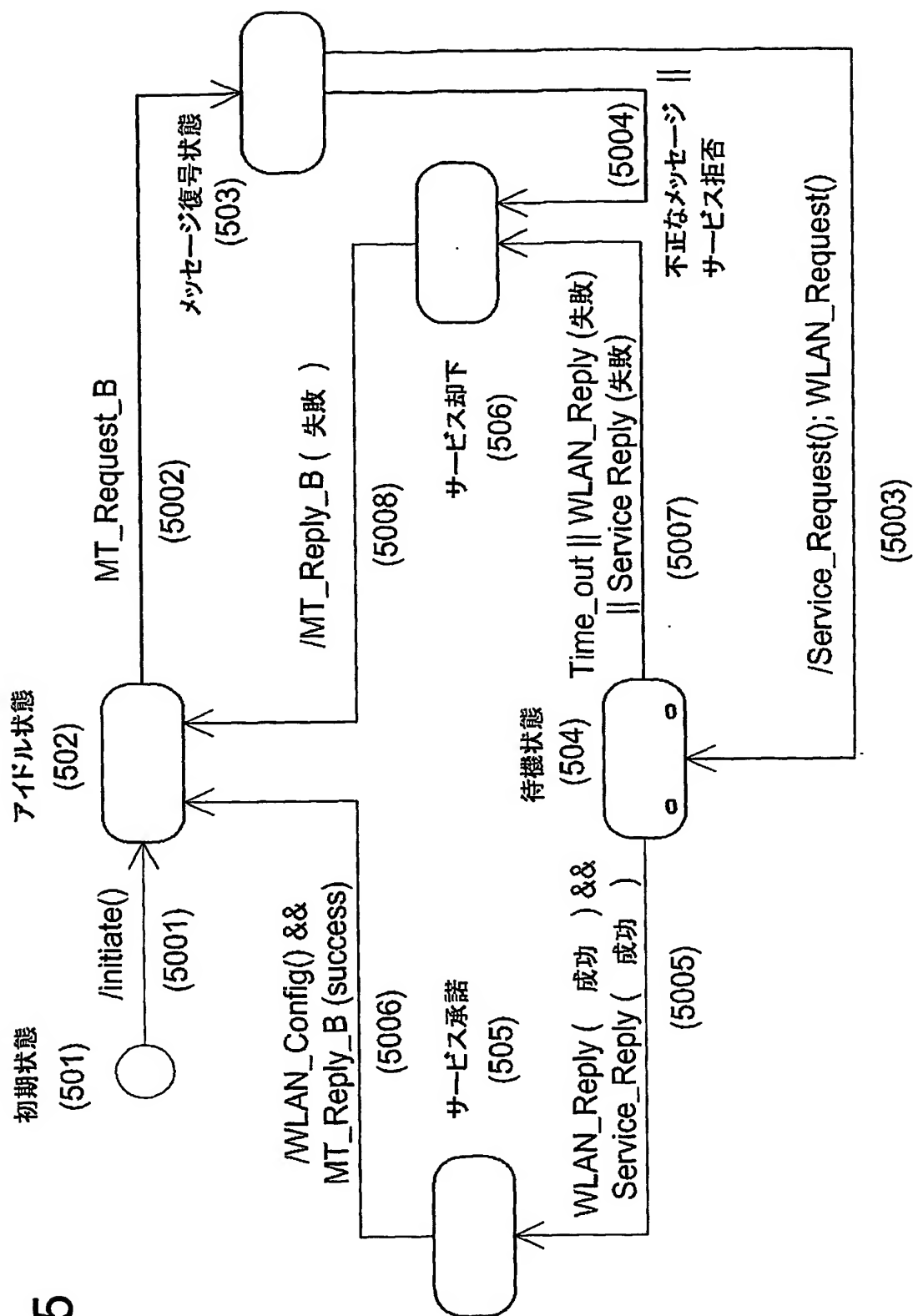


FIG. 6

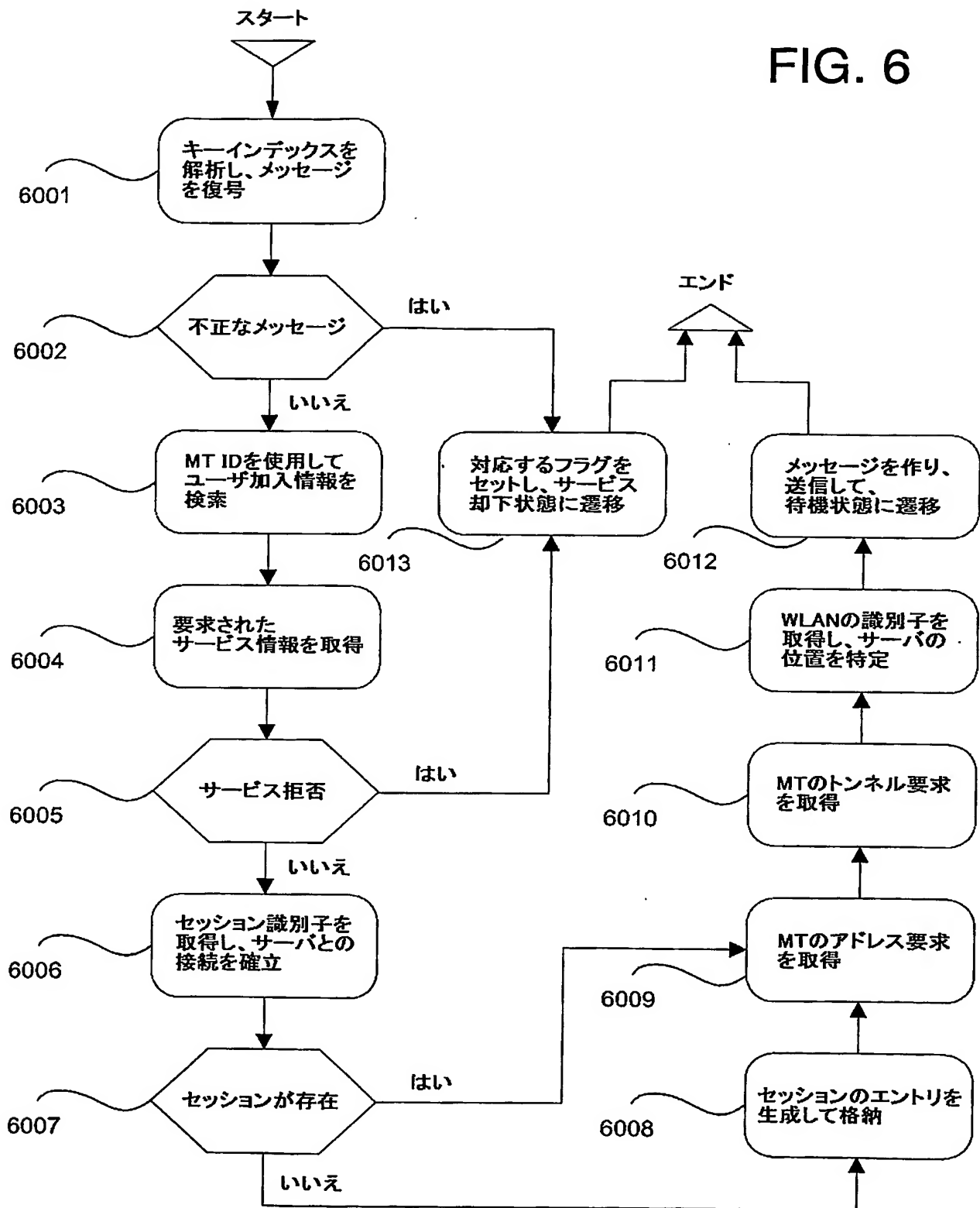


FIG. 7

Home_Network_ID (701)
MT_ID (702)
Session_ID (703)
Address_Request (704)
Service_Spec (705)
Tunnel_Spec (706)
Security_Field (707)

FIG. 8

Home_Network_ID (801)
MT_ID (802)
Address_Alloc (803)
Service_Support (804)
Tunnel_Setup (805)
Security_Field (806)

FIG. 9

Operation (901)
MT_ID (902)
MT_Location (903)
MT_Service (904)
Tunnel_Setting (905)
MT_Address (906)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/000176

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L12/46, H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L12/00-12/66

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 9-55762 A (Nippon Telegraph And Telephone Corp.), 25 February, 1997 (25.02.97), Full text; Figs. 1 to 5 (Family: none)	1-31
A	JP 10-32610 A (NEC Corp.), 03 February, 1998 (03.02.98), Full text; Figs. 1 to 7 & US 6016318 A	1-31
A	JP 2002-94546 A (KDDI Corp.), 29 March, 2002 (29.03.02), Full text; Figs. 1 to 5 (Family: none)	1-31



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T"

later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X"

document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y"

document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&"

document member of the same patent family

Date of the actual completion of the international search

01 April, 2004 (01.04.04)

Date of mailing of the international search report

13 April, 2004 (13.04.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/46Int. Cl⁷ H04L12/28

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L12/00-12/66

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996

日本国公開実用新案公報 1971-2004

日本国実用新案登録公報 1996-2004

日本国登録実用新案公報 1994-2001

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 9-55762 A (日本電信電話株式会社) 1997. 02. 25, 全文, 図1-5 (ファミリーなし)	1-31
A	JP 10-32610 A (日本電気株式会社) 1998. 02. 03, 全文, 図1-7 & US 6016318 A	1-31
A	JP 2002-94546 A (ケイディーディーアイ株式会社) 2002. 03. 29, 全文, 図1-5 (ファミリーなし)	1-31

☐ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの

「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」 口頭による開示、使用、展示等に言及する文献

「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

01. 04. 2004

国際調査報告の発送日

13. 4. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

宮 島 郁 美

5 X

8 5 2 3

電話番号 03-3581-1101 内線 3595